PROGRAMMATIC INTEGRATION OF CYBER INTO THE INSTITUTIONAL DOMAIN OF LEADER DEVELOPMENT

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

DANIEL T. ZIMMER, MAJOR, U.S. ARMY
B.S., The College of Saint Scholastica Duluth, Minnesota, 1993

Fort Leavenworth, Kansas
2015

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
12-06-2015	Master's Thesis	AUG 2014 – JUN 2015

4. TITLE AND SUBTITLE

Programmatic Integration of Cyber into the Institutional Domain of Leader Development

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Major Daniel T. Zimmer, U.S. Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This thesis will assess the institutional domain of leader development in relation to cyberspace education and the implications of poorly integrating cyberspace into leader development. Cyberspace plays an integral role in communications, information, electricity, economics, and our nation's defense. Cyberspace is a great opportunity but it is also a threat. Cybersecurity is one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter. A cross case comparative analysis was used to identify what cyber leader development the Army's Training and Doctrine Command is currently implementing within Army learning institutions, and compare that emerging program to historical cases of other leader development programs created in response to technologies that changed how the Army developed its leaders in the past. The examination of curriculum from Army learning institutions like the Officer Basic Courses, Captains' Career Courses, Intermediate Level Education, and Pre-Command Courses showed that cyberspace has been integrated into Army education to the awareness level only.

15. SUBJECT TERMS
Leader Development, Leader Development Strategy, Integration of Cyberspace, Institutional Domain's Integration of Cyberspace, Cyberspace Curriculum in Army Learning Institutions, Curriculum comparison between Armor, Aviation, and Cyber

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	153	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Daniel T. Zimmer

Thesis Title: Programmatic Integration of Cyber into the Institutional Domain of Leader Development

Approved by:

_____, Thesis Committee Chair
Andrew S. Harvey, Ph.D.

_____, Member
Frank L. Wenzel, M.M.A.S.

_____, Member
Kenneth A. Szmed, Jr., M.M.A.S.

Accepted this 12th day of June 2015 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

PROGRAMMATIC INTEGRATION OF CYBER INTO THE INSTITUTIONAL DOMAIN OF LEADER DEVELOPMENT, by Major Daniel T. Zimmer, 153 pages.

This thesis will assess the institutional domain of leader development in relation to cyberspace education and the implications of poorly integrating cyberspace into leader development. Cyberspace plays an integral role in communications, information, electricity, economics, and our nation's defense. Cyberspace is a great opportunity but it is also a threat. Cybersecurity is one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter. A cross case comparative analysis was used to identify what cyber leader development the Army's Training and Doctrine Command is currently implementing within Army learning institutions, and compare that emerging program to historical cases of other leader development programs created in response to technologies that changed how the Army developed its leaders in the past. The examination of curriculum from Army learning institutions like the Officer Basic Courses, Captains' Career Courses, Intermediate Level Education, and Pre-Command Courses showed that cyberspace has been integrated into Army education to the awareness level only.

ACKNOWLEDGMENTS

I would like to dedicate this thesis to my son, Devon Zimmer. His love of cyberspace and the internet coupled with my strong belief in the Army's leader development strategy helped me develop a topic that I was both interested in and motivated to research. Thank you to my wife for putting up with my long days and weekends and for being a good sport when this thesis conflicted with "the best year of her life." I would also like to thank the following members of Staff Group 23A: Ben Hopper, Ebony Thomas, and Todd Turner—they helped keep me motivated and were good study partners on the many beautiful Saturdays that we spent working on our theses. Thanks is also owed to my committee. Andrew Harvey, Frank Wenzel, and Kenneth Szmed, Jr. helped guide this project and kept me focused and on track. Special thanks to Andrew Harvey for serving as my committee chair. His dedication to this additional duty was appreciated. And finally, thank you to Ann Chapman for proofreading and formatting this research paper to make sure all my I's were dotted and T's were crossed.

TABLE OF CONTENTS

Page

ACRONYMS

ARCYBER	Army Cyber
DOD	Department of Defense
TRADOC	Training and Doctrine Command
USCYBERCOM	United States Cyber Command

ILLUSTRATIONS

Page

TABLES

Page

CHAPTER 1

INTRODUCTION AND OVERVIEW

> The dynamic nature of the 21st-century security environment requires adaptations across the force. The most important adaptations will be in how we develop the next generation of leaders, who must be prepared to learn and change faster than their future adversaries. Simply put, developing these adaptive leaders is the number-one imperative for the continued health of our profession.
>
> —General Martin Dempsey, "Leader Development," *Army*

> Our Senior Leaders are responsible for leading our Army into the future. Cyber should not be a niche; rather everyone should be concerned with the digital operating environment.
>
> —Lieutenant General Rhett Hernandez, Quoted in McFadden, "Fires 2020: Land and Cyber," *Fires*

Leaders within the highest level of our government have included cyberspace in their respective strategies. On October 1, 2010, the Department of Defense (DOD) established the United States Cyber Command (USCYBERCOM). All the services agree that cyberspace is a domain very different from the air, sea, land, and space domains. They also agree cyberspace should be on the same level as the other previously listed warfighting domains because our dependence on networks and cyberspace to conduct daily operations illustrates the importance of addressing the synergies between them.[1] In short, the government, the DOD, and the services are placing increased emphasis on cyberspace. The Army's Training and Doctrine Command (TRADOC) has not placed the same emphasis on developing leaders, within the institutional development domain, capable of dealing with the complexities of future cyber threats. This thesis will assess

[1] Jennifer M. McFadden, "Fires 2020: Land and Cyber," *Fires* (July-August, 2013): 30.

the institutional, operational, and self-development domains of leader development in relation to cyberspace training and education, and the implications of poorly integrating cyberspace into the leader development pillars. In order to examine if TRADOC is not programmatically integrating cyberspace into the leader development domains as effectively as it should in order to combat complex future threats, the following research questions will be used. First and most important, how can the U.S. Army best integrate cyberspace into the education and training pillars of leader development for officers? Second, should cyberspace be included in the institutional, operational, and self-development domains of leader development? Third, at what level should the U.S. Army begin to develop cyber savvy leaders? Finally, do we allow one command, USCYBERCOM, to develop our cyber savvy leaders? This thesis will provide clarity on the topic of leader development as it relates to cyberspace by maintaining a narrow focus on the leader development domains and pillars within the technology of cyberspace.

The cyber threat and cyber technology will be referenced only enough to demonstrate the need for better leader development within cyberspace. It is beyond the scope of this thesis to provide a detailed discussion regarding cyber technology and the complex cyber threat. There are too many nation states, non-nation states, and non-state actors that have the ability to threaten the United States using cyberspace to discuss them here. "Our adversaries are leveraging cyberspace with the potential to place the nation (and the Army) at mortal risk."[2] Additionally, many cyberspace applications, programs, and projects currently conducted by the U.S. military are classified and cannot be included in this thesis. The author is not an expert in cyberspace; nor qualified to discuss

[2] McFadden, 30.

cyberspace infrastructure and its maintenance or conducting offensive and defensive operations within cyberspace. Further, this thesis will not go into detail regarding the manufacture, armament, capability, maintenance, and offensive or defensive use of the tank and Army Aviation unless it pertains directly to a change in leader development relating specifically to that technology.

In order to provide clarity on leader development, cyberspace, and their relationship, chapter 1 of this thesis will define terms related to leader development and cyberspace; define leader development and provide insight into how the Army develops its leaders; define cyberspace and emphasize its importance in operations at all levels; and provide the reader with a basic understanding that cyberspace poses a significant threat to the United States. Chapter 2 will provide the reader a summation of the literature that was used during the research of this paper. Chapter 3 will outline the methodology used to answer the primary and secondary research questions. Chapter 4 will present the findings and the analysis of the research conducted. Chapter 5, the conclusion, will explain to the reader what the answers mean and list recommendations for further research.

Leader Development

Leader development is a deliberate, continuous, sequential, and progressive process grounded in the Army Values. It grows Soldiers and Army civilians into competent, confident leaders capable of directing teams and organizations.[3] Leadership is

[3] Headquarters, Department of the Army, Army Doctrine Reference Publication (ADRP) 7-0, *Training Units and Developing Leaders* (Washington, DC: Government Printing Office, August 2012), 1-2.

the process of influencing people by providing purpose, direction, and motivation to accomplish the mission and improve the organization.[4] The definition of leadership is included in this thesis because it is important to understand that leader development and leadership are linked. In order to develop leaders, good leadership must be practiced. Figure 1, the Army's Leadership Requirements Model shows that one of the competencies of leadership is develops. The Develops subcategory includes prepares self and develops others. For the purpose of this thesis, others will include leaders.

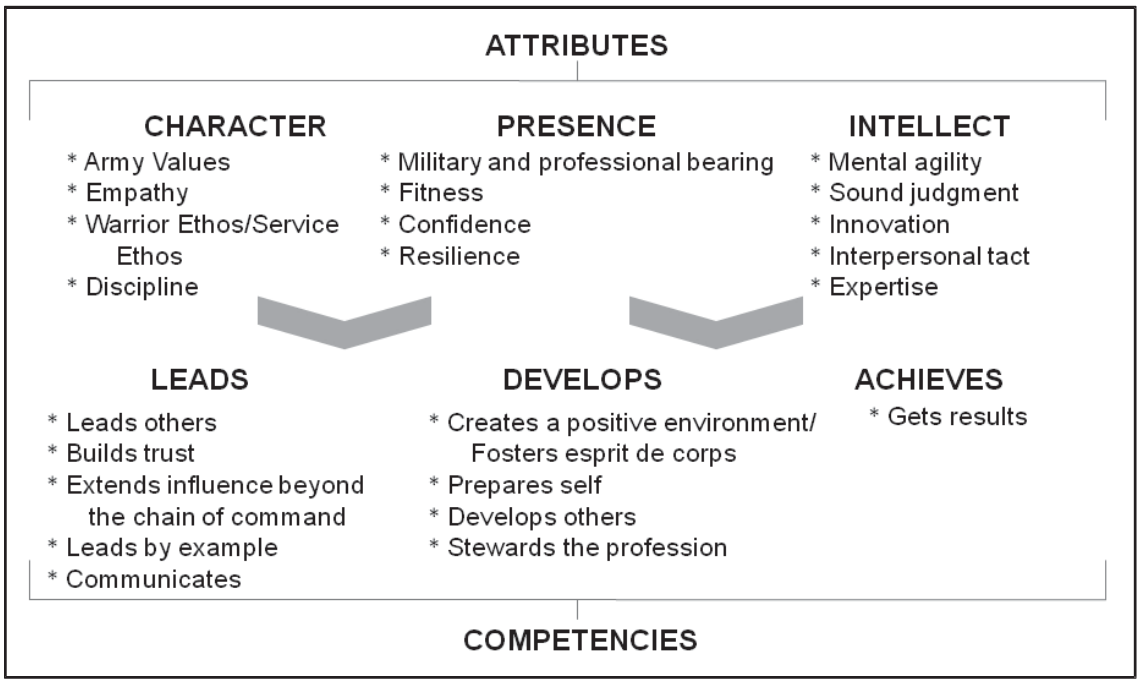


Figure 1. The Army Leadership Requirements Model

Source: Headquarters, Department of the Army, Army Doctrine Reference Publication 6-22, *Army Leadership* (Washington, DC: Government Printing Office, August 2012), 1-5.

[4] Headquarters, Department of the Army, Army Doctrine Reference Publication 6-22, *Army Leadership* (Washington, DC: Government Printing Office, August 1, 2012), 1-1.

Leader development is arguably one of the most important things Army units do when they are not actively engaged in operations.[5] Figure 2 lists the Army's Principles of Leader Development. Once again, we see the link between leadership and leader development. It is clear that Army doctrine supports our senior leaders' emphasis on leader development. In fact, leader development is so important that it is mentioned twice in the Principles of Leader Development. Principle number two is develop subordinate leaders and principle number five is train to develop adaptive leaders. Principles two and five are possibly the most important principles because they clearly illustrate how the Army will prepare its leaders to operate in an uncertain complex future. If the Army's Principles of Leader Development tell leaders what to do with respect to leader development, the Army's model describes how to develop leaders.

- Lead by example.
- Develop subordinate leaders.
- Create a learning environment for subordinate leaders.
- Train leaders in the art and science of mission command.
- Train to develop adaptive leaders.
- Train leaders to think critically and creatively.
- Train your leaders to know their subordinates and their families.

Figure 2. The Army's Principles of Leader Development

Source: Headquarters, Department of the Army, Army Doctrine Reference Publication (ADRP) 7-0, *Training Units and Developing Leaders* (Washington, DC: Government Printing Office, August 2012), 2-4.

[5] Headquarters, Department of the Army, ADRP 7-0, 2-4.

Figure 3, the Army's Leader Ddevelopment Model displays how the Army develops its leaders through three mutually supporting leader development domains.[6] The Leader Development Model illustrates the relationship between the institutional, operational, and self-development domains. The institutional domain is the first of the three domains in which education is the primary pillar. This domain includes but is not limited to, the Army's Infantry Officer's Basic Course, Maneuver Captain's Career Course, and Command and General Staff College. The operational domain is the second of three leader development domains in which training is the primary pillar.

[6] Headquarters, Department of the Army, *Leader Development Strategy* (Washington, DC: Government Printing Office, 2013), 11.

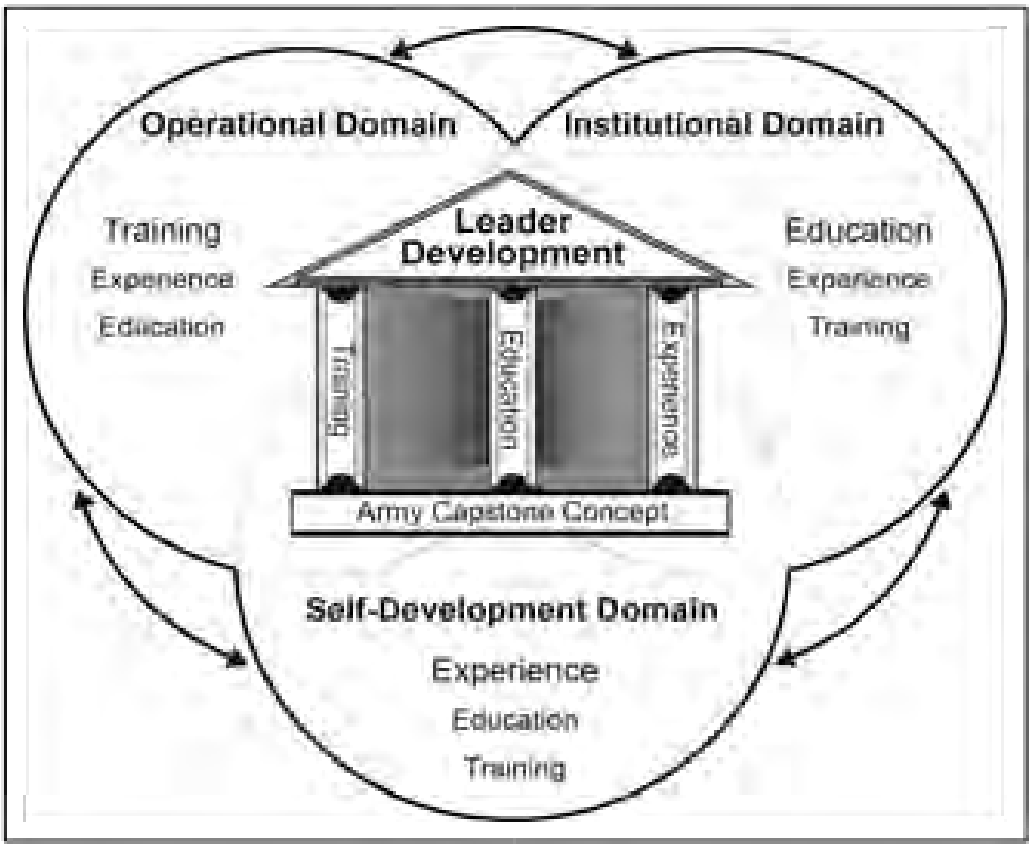


Figure 3. The Army's Leader Development Model

Source: Headquarters, Department of the Army, Army Doctrine Reference Publication (ADRP) 7-0, *Training Units and Developing Leaders* (Washington, DC: Government Printing Office, August 2012), 1-2.

This domain includes operational assignments. The third and final domain, the self-development domain is where experience is the primary pillar. In this domain, the individual leader is responsible for his or her professional development. This domain includes but is not limited to professional development through reading books, journal articles, and/or periodicals.[7] Notice that each domain contains all three pillars. The most important thing to notice about the domains is that they are linked. Each domain does not

[7] Headquarters, Department of the Army, *Leader Development Strategy,* 11.

work within a vacuum but rather takes what another domain has accomplished and builds upon it. The model also depicts three pillars as the center supporting structures to Army leader development. The three pillars are education, training, and experience. Education is the process of imparting knowledge and developing the competencies and attributes Army professionals need to accomplish any mission the future may present.[8] Training is an organized, structured, continuous, and progressive process based on sound principles of learning designed to increase the capability of individuals, units, and organizations to perform specified tasks or skills.[9] Finally, experience is the continuous progression of personal and professional events. It begins before an individual joins the Army and continues after separation.[10] The *American Heritage Dictionary of the English Language* defines a pillar as, "a slender free standing, vertical support, or one who occupies a central or responsible position."[11] The Army's leader development pillars are best described as occupying the central position in the leader development model. One important assumption made in this thesis is that the Army's leader development strategy works. It is beyond the scope of this thesis to attempt to credit or discredit the merits of the Army leader development strategy. For a more detailed description of leader development and how the Army manages it, reference Army Field Manual 7-0, *Training Units and Developing Leaders.*

---

[8] Ibid., 12.

[9] Ibid.

[10] Ibid.

[11] *The American Heritage Dictionary of the English Language*, 3rd ed. (Boston, MA: Houghton Mifflin, 1992), 1373.

Cyberspace

Cyberspace is defined as a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[12] Notice that the definition of cyberspace contains the word domain. For the purposes of this thesis, cyberspace will be treated as a domain similar to the conventional land, maritime, air, and space domains. Although we are labelling cyberspace a domain, it is important to understand that it is substantially different from the conventional domains. The main difference between cyberspace and the conventional domains is that cyberspace is man-made. "Cyberspace is a system of systems in that many small and diverse systems comprise the structure as a whole."[13] Thus, cyberspace is an integral part of all the conventional domains because land, maritime, air, and space based network systems exist. The bottom line is that we depend on cyberspace for almost everything.

Cyberspace plays an integral role in communications, information, electricity, economics, and our nation's defense. Cyberspace is a great opportunity but it is also a threat. President Barak Obama identified cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a

---

[12] Headquarters, Department of the Army, Field Manual (FM) 3-38, *Cyber Electromagnetic Activities* (Washington, DC: Government Printing Office, February 2014), GL-2.

[13] Ibid., 1-5.

government or as a country are not adequately prepared to counter.[14] Our enemies understand this and will use cyberspace to attack our nation. Essye B. Miller, Cybersecurity Director, DOD, Chief Information Office/G6 states, "The Defense Department gets hit with approximately 10 million cyber-attacks each and every day, and a very large number of them are aimed directly at the Army."[15]

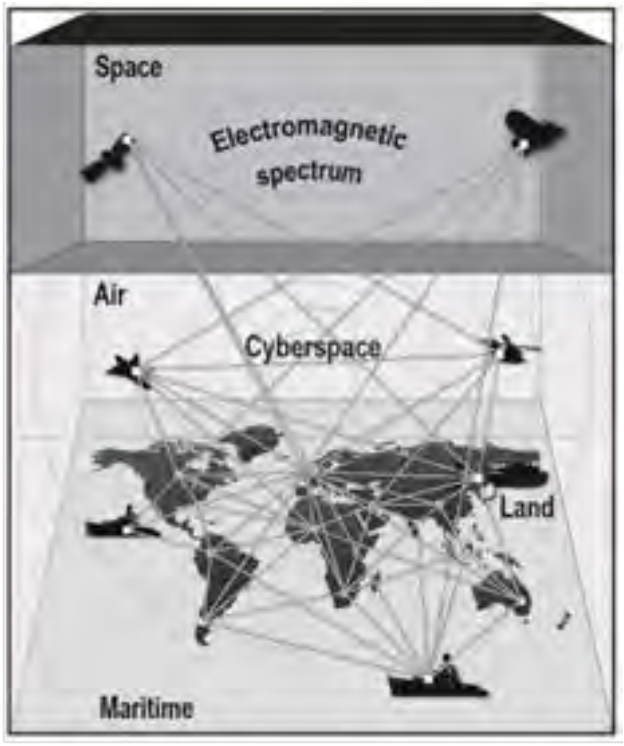


Figure 4. Relationship Among the Five Domains and the Electromagnetic Spectrum

Source: Headquarters, Department of the Army, Field Manual FM 3-38, *Cyber Electromagnetic Activities* (Washington, DC: Government Printing Office, February 2014), 1-4.

[14] U.S. President, "The Comprehensive National Cybersecurity Initiative," The White House, March 2010, accessed October 5, 2014, http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf.

[15] Margaret McBride, "Everyone Critical to Cyber Defense," *Fort Leavenworth Lamp,* October 2, 2014, A2.

Lieutenant General Edward C. Cardon, Commander of USCYBERCOM believes that anything that can pass a one or zero must be considered a weapon.[16] That means that anyone with a computer can conduct an attack against the military's network through cyberspace. In fact, the Internet has sites devoted to providing instructions on how to hack into networks and can teach an individual basic hacking skills in less than twenty-four hours. Two contemporary examples of cyber-attacks are the Shellshock virus and the 2011 Sony attack.

The Shell Shock virus is "a deadly serious bug potentially affecting hundreds of millions of computers, servers and devices . . . that can be used to remotely take control of almost any system using Bash, researchers said."[17] "On April 26, 2011, Sony announced that hackers had broken into its PlayStation and Qriocity networks April 17-19 and may have released the personal and billing information of up to 77 million people . . . Sony reported a second security breach by hackers, who may have stolen personal information of about 24.6 million users on its Sony Online Entertainment site."[18] Even more recently, Sony was hacked again; this time in early November 2014. In the second attack, the hackers stole approximately 100 terabytes of data. "The data included usernames, passwords and sensitive information about its network architecture,

---

[16] Lieutenant General Edward Cardon, Guest Speaker Lecture, U.S. Army Command and General Staff College, Fort Leavenworth, KS, December 3, 2014.

[17] Dave Lee, "Shellshock: 'Deadly Serious' New Vulnerability Found," *BBC News*, September 25, 2014, accessed December 6, 2014, http://www.bbc.com/news/technology-29361794.

[18] Hayley Tsukayama, "Cyber Attack was Large-Scale, Sony Says," *Washington Post,* May 5, 2011, accessed December 6, 2014, http://www.washingtonpost.com/blogs/faster-forward/post/cyber-attack-was-large-scale-sony-says/2011/05/04/AF78yDpF_blog.html.

a list of employee salaries and bonuses; social security numbers and birth dates; human resources employee performance reviews, criminal background checks and termination records, and finally passport and visa information."[19] The Shellshock virus and the Sony attacks are proof that cyberspace can be used maliciously. The Sony attacks prove that it is possible to steal large amounts of personally identifiable information and cause an entire network to be shut down for extended periods of time. The Sony attacks illustrate that cyber-attacks cause mistrust of the network. Additionally, the Sony attacks may have cost Sony billions of dollars. Either attack, if perpetrated against the U.S. military, could be used to infiltrate and take over military systems potentially enabling an enemy to cause severe disruption to the military.

The examples listed above clearly prove that cyberspace is a threat. As cyberspace becomes more complex and barriers of entry continue to drop,[20] it becomes more important than ever that we are doing everything possible to develop agile leaders that can operate within cyberspace.

Definitions

The following cyber electromagnetic definitions are taken from Field Manual 3-38, *Cyber Electromagnetic Activities*. These definitions will help the reader understand that cyberspace can be used offensively and defensively.

---

[19] Kim Zetter, "Sony Got Hacked Hard: What We Know and Don't Know So Far," *Wired,* December 3, 2014, accessed December 10, 2014, http://www.wired.com/2014/12/sony-hack-what-we-know/.

[20] Cardon.

Cyber Electromagnetic Activities: Activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system.[21]

Cyberspace Operations: The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.[22]

Defensive Cyberspace Operations: Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.[23]

Defensive Cyberspace Operation Response Action: Deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend DOD cyberspace capabilities or other designated systems.[24]

Integration: The arrangement of military forces and their actions to create a force that operates by engaging as a whole.[25]

Offensive Cyberspace Operations: Cyberspace operations intended to project power by the application of force in or through cyberspace.[26]

---

[21] Headquarters, Department of the Army, FM 3-38, GL-2.

[22] Ibid.

[23] Ibid.

[24] Ibid.

[25] Ibid., GL-4.

[26] Ibid.

Operational Environment: A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander.[27]

[27] Ibid., GL-5.

CHAPTER 2

LITERATURE REVIEW

The Combined Arms Research Library reference staff at Ft. Leavenworth, KS significantly aided the author in researching U.S. Army's leader development topics. The initial research compilation contained works specifically relating to the Army's leader development programs to include Army doctrine, scholarly works, periodicals, relevant theses, and pertinent monographs. The secondary research request yielded a plethora of sources dealing with cyberspace. Most sources were internet based, but provided extremely valuable information on what cyberspace is, how it is used, why it is a threat, and what the government is doing, militarily and within the civilian sector, to combat the cyber threat. The following paragraphs will break down all the material accessed during this research project and provide the reader with a brief summary of said material.

The published and unpublished sources provided a plethora of information on leader development but did not yield very much for cyberspace. These sources did not provide any detailed information on the Army leader development model's institutional domain in regards to cyberspace. However, these documents did help define relationships between the pillars of leader development, illustrate that leader development is a continuous and iterative process and that the pillars do not always lead to a 1 to 1 to 1 = leader developed ratio.[28] In other words, leader development is not just a recipe that produces the same product when we add the same exact amount of ingredients to the mix. Every leader is different and may require more interaction within a certain pillar or

[28] Mr. Frank Wenzel, conversation with author, Ft. Leavenworth, KS, October 16, 2014.

combination of pillars. Leader development is a conceptual model that the Army's senior leaders are very interested in. General Raymond Odierno states, "We must develop leaders with the breadth and depth of experience necessary to meet tomorrow's demands."[29] "Developing Leaders" by Frank Wenzel, Chief of the Army Leader Development Division in the Center for Army Leadership, Fort Leavenworth, Kansas, expertly defines leader development and stresses that it is, again, an iterative process. The White Paper clearly explains the relationships between the education, training, and experience leader development pillars and how they inter-relate within the three leader development domains. Figure 5 displays how the leader development pillars can be treated as lines of effort. Notice that each line of effort, or pillar, passes through each of the leader development domains. This diagram simply shows that each pillar or line of effort is occurring within each of the domains. What this diagram does not display effectively is that each domain has a primary focus. The institutional domain for example includes schools like the Infantry Officer's Basic Course, the Armor Officer's Basic Course, the Command and General Staff College, and the Army War College. The institutional domain also includes Army basic training. Even though this domain includes both training and education, education is the primary focus. The operational domain also includes all three pillars, or lines of effort, but its focus is training. A leader receives education and gains experience during operational assignments but, operational assignments primarily train and develop agile leaders through challenging scenarios.[30]

---

[29] General Raymond T. Odierno, Keynote Speech, Association of the United States Army Annual Eisenhower Luncheon, October 23, 2013.

[30] Headquarters, Department of the Army, *Leader Development Strategy,* 11-12.

Finally, the self-development domain's main focus is experience. This domain allows a leader to use his or her experience as a base and seek external growth opportunities. Experience allows a leader to determine what, specifically, they need to develop. The Army's Leader Development Strategy's framework "is a mutually shared responsibility between the institutional Army (education or training institution), the operational force (organization or unit), and the individual."[31]

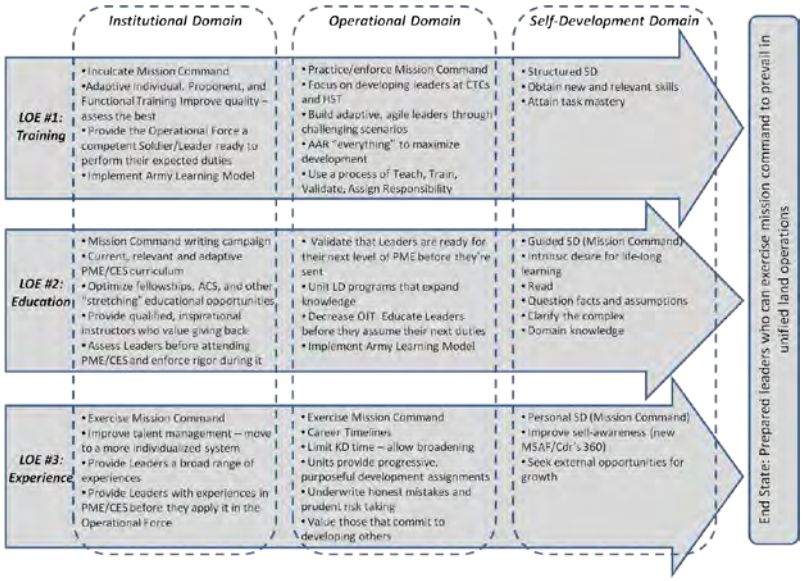


Figure 5. Illustration of the Three Leader Development Pillars Represented as Lines of Effort

Source: Headquarters, Department of the Army, *Leader Development Strategy* (Washington, DC: Government Printing Office, 2013), 10.

[31] Headquarters, Department of the Army, *Leader Development Strategy*, 6.

The doctrinal and theoretical sources sampled provide many of the cyber and leader development definitions and diagrams used in this thesis. The definitions and diagrams will help readers understand the terminology and the relationship between terms. For example, leadership development and leader development are not the same thing, yet are often used interchangeably. They are two very different processes that are linked together. Army Doctrine Reference Publication 6-22, *Army Leadership* outlines leadership and Army Doctrine and Reference Publication 7-0, *Training Units and Developing Leaders* provides the framework and limitations for leader development. The 2013 Army *Leader Development Strategy* provides the ends, ways, and means or more simply, the final goal, the how, and with what resources we should use.

Cyberspace doctrinal references provided the author with a basic understanding of what cyberspace is. The cyber publications explained the relationship between cyberspace operations and the electro-magnetic spectrum and how they are related. Figure 6 explains that cyber operations, electronic warfare, and spectrum management operations are each conducted within the electromagnetic spectrum and consistently overlap. The overlapping is what is referred to as cyber electromagnetic activities.

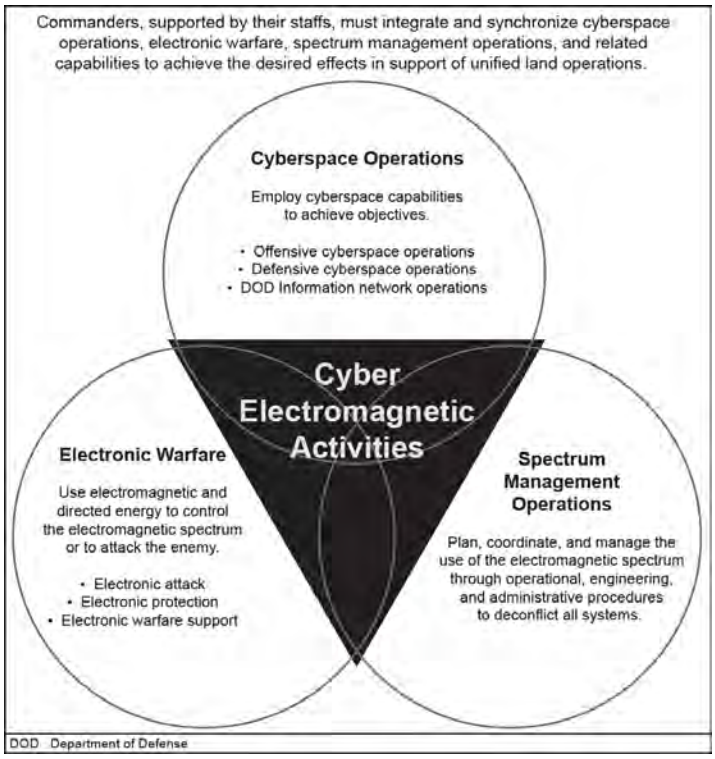


Figure 6. Depiction of Cyber Electromagnetic Activities

Source: Headquarters, Department of the Army, Field Manual 3-38, *Cyber Electromagnetic Activities* (Washington, DC: Government Printing Office, February 2014), 1-2.

The Army Field Manual 3-38, *Cyber Electromagnetic Activites* confirms that offensive and defensive operations can be conducted within cyberspace. Additionally, the field manual provided the author with a visual representation of the five operational domains: land, sea, air, space, and cyberspace and how they are all related. Unfortunately, Field Manual 3-38 was the only piece of unclassified cyber doctrine available at the time this thesis was researched. On December 3, 2014, in a lecture to the 2015 Command and General Staff College class, Lieutenant General Edward Cardon briefly mentioned that because cyberspace and the cyber threat are changing rapidly it is difficult to publish

timely doctrine that is also relevant. Lieutenant General Cardon's lecture on cyberspace put into perspective the complexity of cyberspace and the threat it presents to the DOD and the civilian sector. He also discussed, in no great detail, what types of cyber units or cyber teams were being created to combat the cyber threat. Lieutenant General Cardon specifically listed the vulnerabilities to cyberspace as: (1) improper architecture; (2) poor patching; and (3) poor user practices.[32] Cyber architecture is created by humans, patches are created by humans, and users are human. Therefore, all three vulnerabilities are either directly or indirectly influenced by human beings. If the last statement is true, it stands to reason that developing adaptive and agile leaders within the cyber domain should be a priority. Developing adaptive and agile leaders is important because leaders must know how to train and educate subordinates to decrease the listed vulnerabilities. Additionally, leaders must also have the experience to know what self-development tools are available to them and their subordinates to ensure that the listed vulnerabilities are, again, decreased. Finally, leader development principles two, three, five, and six can directly help decrease the three cyberspace vulnerabilities. A limiting factor to researching military and cyberspace was that the majority of the Army's cyber program is classified Top Secret or higher. Subsequently, no research was conducted beyond what was available from unclassified sources. Not surprisingly, there was substantially more unclassified material available regarding cyberspace, cyber infrastructure, and the cyber threat published by civilians and civilian companies.

The 2012 *National Defense Strategy*, the 2010 and 2014 *Quadrennial Defense Reviews*, and the 2012 *National Military Strategy of the United States of America*

[32] Cardon.

illustrate that senior leaders have made cyberspace, and its defense, a priority for our military forces. These sources support the argument that there is a need for leader development within cyberspace. The 2010 *Quadrennial Defense Review* analysis strongly suggests "that the Department of Defense must further rebalance its policy, doctrine, and capabilities to better support one of six key missions - operating effectively in cyberspace."[33] Additionally, these documents are in agreement that it is important for the DOD to continue to develop leaders that are able to conduct operations in an uncertain complex future.[34] There needs to be a connection between identifying cyberspace as a significant threat and the importance of developing leaders for an uncertain tomorrow. It is clear that the uncertain tomorrow will include cyberspace and therefore the Army must better develop its leaders to deal with the increasingly complex cyber threat. This is supported by the 2014 *U.S. Army Operating Concept*. The central idea of the *Operating Concept* is, "Army forces defeat enemy organizations, control terrain, secure populations, consolidate gains, and preserve joint force freedom of movement and action in the land, air, maritime, space, and cyberspace domains."[35] The *Army Operating Concept* lists "Develop innovative leaders and optimize human performance" as one of ten ways the Army will use to accomplish its central idea.[36]

---

[33] Robert M. Gates, *Quadrennial Defense Review* (Washington, DC: Defense Department, 2010), 2.

[34] Ibid., xiii.

[35] Department of the Army, Headquarters U.S. Army Training and Doctrine Command, Training and Doctrine Command Pamphlet 525-3-1, *The U.S. Army Operating Concept: Win in a Complex World 2020-2040* (Fort Monroe, VA: Government Printing Office, October 2014), 17.

[36] Ibid., 20.

The internet provided a large quantity of electronic sources that helped further define cyberspace and provided information on what the civilian sector is doing to develop their cyber leaders. The bottom line is that the civilian sector has an advantage in recruiting and retaining talent over the military because they can offer larger salaries. The civilian sector is reporting that their workforce is very capable when it comes to cyber technology and management but not both at the same time. One electronic source described the need for cyberspace courses similar to the Army's Ranger School. "A Cyber Leader Course of similar duration and intensity to Ranger School, but tailored to cyber operations would help fill the critical shortage of technically and operationally competent cyber leaders."[37] The United States Military Academy (West Point) provided a number of online reports detailing the need for cyber leader courses. Lucas Kagel, Chief of Concepts and Doctrine for USCYBERCOM explains that the command wants "to incorporate cyberspace leader development at all levels of professional military and civilian education."[38] Mike Milord's article "Leader development a critical part of cyberspace mission" illustrates that the USCYBERCOM understands that cyber leader development must occur throughout the Army, not just within the cyber commands. Milord states, "This will ensure the Army has sufficient planners and leaders with

[37] Gregory Conti, Michael Weigland, Ed Skoudis, David Raymond, Thomas Cook, and Todd Arnold, "Towards A Cyber Leader Course Modeled on Army Ranger School," *Small Wars Journal* (April 18, 2014), accessed October 9, 2014, http://smallwarsjournal.com/jrnl/art/towards-a-cyber-leader-course-modeled-on-army-ranger-school.

[38] Mike Milord, "Leader Development a Critical Part of Cyber Space Mission," U.S. Army, August 9, 2012, accessed September 21, 2014, http://www.army.mil/article/85408/Leader_development_a_critical_part_of_cyberspace_mission.

knowledge to integrate cyber capabilities into the combatant commander's operations and planning."[39]

Army Cyber Institute published a number of reports that discuss, in detail, the need for "unique, demanding, and immersive training that fills a necessary gap in Army cyber leader development."[40] One report, titled *Towards a Cyber Leader Course: Not for the Weak or Faint Hearted*, *Professionalizing the Army's Cyber Officer Corps*, and *A Proposed Army Information Dominance Officer Education Model* discuss subjects ranging from creating a cyber-leader's course that is modeled after the Army's elite Ranger course to replacing the Army's Signal Corps, Military Intelligence Corps, and the Electronic Warfare functional area with an all-inclusive Cyber Corps. These reports, supported by information provided by Lieutenant General Cardon, propose that cyberspace can be represented by physical terrain and that the military can train within it exactly like Infantry Soldiers would train inside a Military Operations inside Urban Terrain site. Figure 7 represents how cyberspace is depicted for training purposes. Each street or structure represents an information pathway, node or piece of a cyber-network that can be attacked or defended. Figure 8 depicts a Military Operations in Urban Terrain site and figure 6's CyberCity. Figures 7 and 8 offer overhead visual depictions of terrain and when viewed side by side, the similarities are very apparent. It can be argued that an overhead view or a vantage from high ground helps provide a clearer common operating

---

[39] Milford.

[40] Gregory Conti, Michael Weigland, Ed Skoudis, David Raymond, Thomas Cook, Todd Arnold, and Daniel Ragsdale, *Towards a Cyber Leader Course: Not for the Weak or Faint of Heart* 1337, no. 3 (May 2014), accessed October 13, 2014, http://www.westpoint.edu/acc/SiteAssets/SitePages/Reports/FULL_TCLC.pdf.

picture to leaders. Lieutenant General Rhett Hernandez states, "education, training, and experience are key to understanding the threat, and the cyberspace terrain."[41] Notice the connection between the leader development pillars and what senior Army leaders are discussing regarding cyberspace.

Figure 7. CyberCity

Source: Gregory Conti, Michael Weigland, Ed Skoudis, David Raymond, Thomas Cook, Todd Arnold, and Daniel Ragsdale, *Towards a Cyber Leader Course: Not for the Weak or Faint of Heart* 1337, no. 3 (May 2014): 5, accessed October 13, 2014, http://www.westpoint.edu/acc/SiteAssets/SitePages/Reports/FULL_TCLC.pdf. This is a small scale mock-up of a city, including its key underlying computing, networking, and critical infrastructure systems using real-world back-end components.

[41] McFadden, 30.

Figure 8. Military Operations on Urban Terrain

Source: Gregory Conti, Michael Weigland, Ed Skoudis, David Raymond, Thomas Cook, Todd Arnold, and Daniel Ragsdale, *Towards a Cyber Leader Course: Not for the Weak or Faint of Heart* 1337, no. 3 (May 2014): 5, accessed October 13, 2014, http://www.westpoint.edu/acc/SiteAssets/SitePages/Reports/FULL_TCLC.pdf, 5. Military Operations on Urban Terrain environments could be integrated with the CyberCity concept to create an ideal training and evaluation environment for a Cyber Leader Course.

Cyber-attacks are real and could have devastating effects on our communications infrastructure, banking and economy, electrical grids, and security systems. Another recent example is a virus called Stuxnet. In 2010, it infected the nuclear centrifuges within one of Iran's nuclear facilities. In this particular case, Stuxnet's effect was non-life threatening. It is possible however, that with manipulation, Stuxnet or one like it, could damage a more vital system causing a melt down and ultimately a nuclear disaster.[42]

[42] Sandra@F-Secure, "Computer Invaders: The 25 Most Infamous PC Viruses of All Time," Safe and Savy, March 21, 2011, accessed October 29, 2014, http://safeandsavvy.f-secure.com/2011/03/21/25-infamous-viruse/.

In a byline published by States News Service, Bill Ackerly reports that senior Army leaders met at an Association of the United States Army Mission Command Symposium on June 19, 2012 and discussed questions like "Are we doing the right thing? Do we have the right people involved?"[43] Alan Paller, co-founder of CyberAces nonprofit, and chair of a Department of Homeland Security task force on cyber job vacancies, says that the U.S. Army is currently doing a good job on recruiting and training cyber defense personnel.[44]

The August, 2014 issue of *National Defense* published an article that discussed the importance of developing cyber talent from within. The article mentions an aptitude test that the USCYBERCOM has developed to find cyber savvy Soldiers. The article goes on to say, one of the pitfalls of investing time and money into developing cyber leaders is that the military cannot compete with civilian sector salaries.[45] Lieutenant General Cardon stated that one way to manage talent and retain cyber savvy warriors is to publicize that you get to have all the same fun that hackers do, but in the Army it is legal.[46]

The last document that offers some credence to the importance of developing cyber savvy leaders is the DOD's Cyberspace Workforce Strategy. In this document, the DOD outlines a plan with the following six focus areas: (1) establish a cohesive set of

---

[43] Bill Ackerly, "Lawrence Says Everything is Network Dependent," *States News Service*, June 20, 2012.

[44] Stew Magnuson, "Cyber Labor Shortage Not What It Seems, Experts Say," *National Defense* (August 2014): 30-31.

[45] Ibid.

[46] Cardon.

DOD-wide cyberspace workforce management issuances; (2) employ a multi-dimensional approach to recruiting; (3) institutionalize continuous learning with greater focus on evaluating the maturity of skills; (4) retain qualified personnel; (5) expand the threat knowledge; and (6) understand crisis and surge requirements and options.[47] For this thesis, the biggest takeaway is that the DOD acknowledges cyberspace is a threat and has begun to implement a plan for developing cyber savvy leaders. This document places emphasis on cyber savvy warriors operating within the respective cyber commands and not so much within the general Army force. It can be argued that, at the very least, focus areas (1), (4), (5), and (6) need to be understood and utilized by the entire Army force in order to better protect the networks and maintain our freedom to operate within cyberspace.

The literature used during this research confirmed the author's concern that our future leaders will need to be better trained in cyberspace and its applications. From the President to the Secretary of Defense to the Chairman of the Joint Chiefs of Staff to senior Army leaders at the operational level there is an agreement that cyberspace is a great opportunity but at the same time is a complex threat to the United States. The President's May, 2010 National Security Strategy states that the United States will continue to invest in capabilities that will allow us to prevail in all domains including the cyber domain.[48] The Secretary of Defense and the Chairman of the Joint Chiefs of Staff

---

[47] U.S. Department of Defense, *Department of Defense Cyberspace Workforce Strategy,* Chief Information Officer, U.S. Department of Defense, December 4, 2013, accessed October 13, 2014, http://dodcio.defense.gov/Portals/0/Documents/DoD%20Cyberspace%20Workforce%20Strategy_signed(final).pdf.

[48] U.S. President, *National Security Strategy of the United States* (Washington, DC: The White House, May 2010), 22.

also nest the importance of cyberspace in their strategic level documents; the *Quadrennial Defense Review* and the *National Military Strategy of the United States of America* respectively. There is commitment at senior leader level to do what it takes to fight and win in cyberspace. Is TRADOC doing everything necessary to ensure we can fight and win in cyberspace?

This study will identify some of the potential implications of an inadequate focus on cyberspace training, education, and experience within our leader development domains. This thesis will examine curriculum from institutional organizations across the army to assess the amount and focus of cyber leader development.

CHAPTER 3

METHODOLOGY

This chapter outlines a cross case comparative analysis used to examine the cyber leader development TRADOC is currently implementing within Army learning institutions, and compare that emerging program to historical cases of other leader development programs created in response to technologies that changed how the Army developed its leaders in the past. Points of comparison will be in the Army's leader development pillars and the leader development domains themselves which will serve as the metrics to either prove or disprove the hypothesis of this research paper.

It is critical that the reader remember that the Army's leader development model consists of the institutional, operational, and self-development domains. Each domain contains three leader development pillars. Although each domain contains all three pillars, one of the pillars in each is the main focus. For example, the institutional domain contains the education, experience, and training pillars but the domain's primary focus is on education (see figure 3).

As this thesis previously stated, the institutional domain utilizes programs like the Infantry Officer's Basic Course, the Armor Officer's Basic Course, the Maneuver Captain's Career Course, and the Command and General Staff College as methods to develop leaders through education. Using credit or class hours as a metric, it is possible to determine if leaders within these Army institutions are receiving cyberspace education. For example, if cyberspace education is not offered in the curriculum, it can be deduced that TRADOC is not placing emphasis on developing leaders capable of operating within cyberspace.

The operational domain's primary pillar is training. The Army trains leaders in a variety of ways. Commissioned Army leaders receive initial training during commissioning courses such as the Reserve Officer Training Corps, Officer Candidate School, and assorted military academies. Subsequent branch specific training occurs at one of the many different officer basic courses. Once commissioned, an Army leader is assigned to an operational unit and receives additional unit and job specific training. Upon completion of most, if not all, training courses, the individual receives a certificate of training and the officer's record brief is updated to reflect course completion or training hours completed. A few examples are the Mortar Leader's Course, the Bradley Leader's Course, Combatives Level I thru IV, and Airborne School. Training course completion and training hours completed entries on officer record briefs can be used as metrics to prove or disprove the effectiveness of leader development within the operational domain.

The self-development domain's primary pillar is experience. Although experience is gained within the institutional and operational domains, experience plays the largest role during self-development. Measuring the effectiveness of the self-development domain is more difficult than the operational and institutional domains because leader development within this domain falls upon the individual rather than the Army. However, degrees or certificates earned from formal or web-based courses completed on an individual's personal initiative, and outside the institutional or operational Army, could be considered metrics for confirming or denying the effectiveness of this domain.

Each domain therefore has a metric that can be used to measure the effectiveness of leader development within that specific domain. To summarize these, the metrics

include credit hours, training courses or hours completed, and external degrees or certificates earned.

The hypothesis of this research is that TRADOC has not programmatically integrated cyberspace into the leader development domains as effectively as it should in order to combat complex future threats. The null hypothesis is that TRADOC has programmatically integrated cyberspace into the leader development domains as effectively as it should in order to combat complex future threats.

This thesis will disprove (reject) the null hypothesis by demonstrating that TRADOC is not integrating cyberspace into leader development as effectively as it should. It will also show that there may be better methods of integration available based on previous changes to leader development programs. The technological changes used for comparison of leader development programs are the introduction of the tank and aircraft. The introduction of these technologies caused the Army to develop two new branches—Armor and Aviation. Additionally, the Army was forced to make changes in how they developed leaders. For example, after the tank, the airplane, and the helicopter were introduced, the Army developed and implemented officer basic courses, career courses, and advanced leader courses for both branches. Available cyber curriculum and courses within the Signal Career Course will also be examined to discover what emphasis is being placed on cyber leader development within that specific career course. Changes in tactical Army doctrine, development of specific schools, and additions to curriculum will also be used as metrics to compare cases.

The Army leader development pillars and domains along with changes in doctrine, development of new schools, and additions to curriculum in existing schools are

potential points of comparison for this thesis. Although quantifiable metrics for each pillar have been identified, it is necessary to narrow the scope of this thesis even further by de-limiting the metrics for the operational and self-developmental domains and their focus pillars of training and experience respectively. Due to the time constraints associated with conducting in-depth human subject research—sampling officer record briefs and transcripts, and the issues associated with safe handling of Personally Identifiable Information,[49] this thesis will only examine the institutional domain with a focus on education. Changes in doctrine, the development of specific schools, and the revision or addition of curriculum to existing schools will be the metrics used to compare cases. The metrics for the education pillar will remain institutional curriculum. Curriculum from Officer Basic Courses, Captains' Career Courses, Intermediate Level Education Courses, School of Advanced Military Studies, and Pre-Command Courses can be sampled and compared without compromising Personally Identifiable Information.

The primary source material for the institutional domain is taken from the Army's Centers of Excellence home pages, the Armor and Aviation Schools' Program of Instruction memorandums, curriculum provided by the Intermediate Level Education, Captain's Career Course, Pre-Command Course, and the School of Advanced Military Studies program managers.

[49] The Department of Homeland Security defines personal information as "any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department." The Privacy Office, Homeland Security, "How to Safeguard Personally Identifiable Information," U.S. Department of Homeland Security, Washington, DC, May 2011.

The research process will consist of three main phases. The first phase consists of the collection and selection of data and information. The second phase will identify methods and criteria for the assessment process and will present the results of the cross case comparison. In the final phase, collected data and information will be compared, analyzed and a clear and concise conclusion will be proposed.

This thesis applies the following metrics to evaluate the integration of cyberspace subject matter understanding into the Army's overall leader development strategy. The institutional domain, with education as its focused pillar, will use credit or class hours earned within Army learning institutions. Changes in doctrine, development of specific schools, and additions to curriculum will also be used as metrics.

Three secondary research questions were posed in chapter 1. Should cyberspace be included in the institutional, operational, and self-development pillars of leader development? At what level should the Army begin to develop cyber savvy leaders? Do we allow one command, USCYBERCOM, to develop our cyber savvy leaders? The three questions listed above will be addressed by analyzing a Capabilities Based Assessment conducted by Army Cyber Command and the education agreement between the Command and General Staff College and Kansas State University.

CHAPTER 4

ANALYSIS

The purpose of this research is to investigate whether TRADOC is programmatically integrating cyberspace into the leader development domains as effectively as it should in order to combat complex future threats. As previously discussed in the introduction of this thesis, the President of the United States considers cyberspace to be a threat. The Secretary of Defense iterates the President's concern and also lists cyberspace as a threat within the *National Defense Strategy*. The subordinate strategic documents including the *Quadrennial Defense Review* and the *National Military Strategy of the United States of America* both list cyberspace as a threat and also discuss methods of developing leaders capable of combatting future complex threats. This research was conducted because the author did not feel that the U.S. Army was placing an appropriate emphasis on developing cyber savvy leaders within the institutional domain's education pillar. This research compares previous cases of major changes in the institutional domain's education pillar in response to new technology.

The cross case comparative analysis methodology allowed the author to identify what cyber leader development TRADOC is currently implementing within Army learning institutions, and compare that emerging program to historical cases of other leader development programs created in response to technologies that changed how the Army developed its leaders in the past. This thesis identified the Army's Armor and Aviation branches to serve as the historical cases the author will use to compare the Army's emerging cyber program. Armor and Aviation were chosen because they each presented the Army with an emerging technology that forced the Army to change or

create new doctrine as well as form institutions that would develop leaders capable of employing the new emerging technologies.

As a reminder, the primary research question of this thesis is: Is the Army Training and Doctrine Command programmatically integrating cyberspace into the leader development domains as effectively as it should? The three secondary questions proposed in this research are: (1) Should cyberspace be included in the, institutional, operational, and self-development pillars of leader development?; (2) At what level should the U.S. Army begin to develop cyber savvy leaders?; and (3) Do we allow one command, USCYBERCOM, to develop our cyber savvy leaders? The answers to these questions will be explored in chapter 5 where the author will interpret the findings, provide meaning, present the conclusion for this research, and make recommendations for further study.

In order to use a cross case comparative analysis methodology, two major technological changes incorporated by the Army were selected as comparative cases. The following sections will discuss the Army's Armor and Aviation branches. First, this chapter will provide the background information the reader needs to understand how and why both branches were formed and what changes were made to Army doctrine to compensate for the emergence of the tank and the helicopter. Second, this chapter will discuss the development of branch specific schools specifically created to develop the leaders within those branches. Third, this chapter will provide the reader details on the curriculum from some of the Army's learning institutions in order to determine if the Army has programmatically included cyberspace into the institutional domain's education pillar of leader development as effectively as it could be. The Army learning

institutions examined are the Officer Candidate School, the Infantry Officer's Basic Course, the Maneuver Captain's Career Course, the Command and General Staff College's Intermediate Level Education, the School of Advanced Military Studies, and the Pre-Command Course.

Similarities exist between the creation of the Aviation branch, and the Armor branch during the interwar period, and the creation of the cyberspace branch in 2014. Aviation, Armor, and cyberspace all were originally considered opportunities. The pro-Armor community believed that armor offered the opportunity to make attrition style warfare obsolete. German innovations in armor during the interwar period threatened the United States. This perceived threat forced the United States to change doctrine and educate its leaders differently than before. Aviation was initially used as a method to pass over enemy fortified lines and attack the enemy's rear areas. Army Aviation was also used for reconnaissance. The introduction of both armor and aviation technologies caused significant changes in doctrine and education of Army leaders.

Before examining armor and aviation and the changes to doctrine and leader development their introduction caused, it is important to understand the relationship between doctrine and leader development.

> Since doctrine is that which is officially approved to be taught, it provides the primary content of the curriculum of the Army school system. Doctrine also assists in the development of organizations and weapons systems; it establishes the potential functions of the various systems and the parameters under which units are organized.[50]

---

[50] Major Robert A. Doughty, Leavenworth Papers No. 1, *The Evolution of US Tactical Doctrine 1946-76* (Fort Leavenworth, KS: Combat Studies Institute, August 1979), 1.

In other words, changes in doctrine drive what and how we teach within Army education institutions. The next few sections will provide the reader with a brief historical summary of the introduction of both the tank and Army aircraft.

The U.S. Armor branch traces its origins to the Cavalry and the innovations that occurred during the interwar period. The Tank Service was formed on March 5, 1918.[51] The Armored Force was formed later on July 10, 1940.[52] Armor became a permanent branch of the Army in 1950.[53] The U.S. Armor School was established in October of 1940, just before our country entered World War II.[54] From the formation of the U.S. Tank Service, it took just over twenty-two years to form a school specifically designed to train Army leaders on tank doctrine, tactics, techniques, and procedures. The first Army Armor Officers' Basic Course was run shortly after the opening of the Armor School. The Armor School at Fort Knox, Kentucky was responsible for establishing armored formations, doctrine, and training in the use of armored vehicles. The United States was slow to develop its own armored doctrine. Initially, the United States borrowed tank design and doctrine from the British and French. The British used heavy tanks to penetrate lines and crush resistance while the French used light tanks to support infantry elements. The United States adopted both methods for using tanks.[55] The use of the tank

---

[51] Armor Branch Historian, "The Heritage of Armor-Horse Cavalry Roots," U.S. Army Maneuver Center of Excellence, November 25, 2014, accessed March 1, 2015, http://www.benning.army.mil/armor/historian/.

[52] Ibid.

[53] Ibid.

[54] Ibid.

[55] Armor Branch Historian, "The Heritage of Armor-Horse Cavalry Roots."

during World War I was primarily for the shock and awe effect on infantry forces. Large tank formations could not be used effectively because of the limited ability to command and control the formations.[56] The United States struggled to develop doctrine during the interwar period. After World War I, the United States passed its National Defense Act of 1920 which redefined how the Army was organized and how it was to operate. Specifically, it gave the exclusive responsibility for tank development, training, and doctrine to the Infantry.[57] Because the Infantry's mission was to seize and hold ground, it also became the tank's mission. The bottom line is that the formation of the Armor branch and the changing purpose of armor caused the U.S. Army to write and re-write new doctrine.

Post World War II Armor studies detailed that Armor was best used as an Infantry support platform. Armor could be used to break through enemy lines but the Infantry would seize and hold the ground for future exploitation. Thus, the tank and its development remained under Infantry control until 1950 when it became its own independent branch. From the end of World War I until 1950, tank doctrine dictated that first, the tank is the best anti-armor weapon and should be deployed as such and second, the tank or formations of tanks should never be deployed independently. The tank must support other combat arms. [58] Armor and Infantry officers were taught how to deploy Armor and Infantry together in order to effectively mass, seize, and exploit the initiative. This can be considered the birth of U.S. combined arms doctrine. Between the end of

[56] Ibid

[57] Ibid

[58] Doughty, 5.

World War II and the Korean War U.S. tactical doctrine remained offensive in nature.[59]The Korean War forced the United States to modify its doctrine and begin to focus on defensive operations.[60] The tank combined with Infantry, Field Artillery, and Aviation no longer spread itself along a thin front to repel enemy attacks. Defensive doctrine was developed that incorporated the tank into an area defense or mobile defense in which it was used as a mobile strike platform to repel an enemy penetration. In order to prevent disorderly high casualty producing withdrawals, retrograde operations doctrine was modified and taught to leaders in the school houses.

During the 1950s, the U.S. Army doctrine limited mobility for increased fire power. Although the tank was sometimes used as a mobile strike platform, it was employed mainly in the static defense. It was heavily dug in and sometimes used as an indirect fire weapon system. In Korea, units learned that small teams of infantry and tank units spread throughout the valleys and the high ground prevented the enemy from effectively ambushing or enveloping U.S. forces.[61]

The 1960s brought more changes to tank doctrine and education development of U.S. Army leaders. During Vietnam, tanks were used during sweep missions, jungle busting operations, and thunder runs. This doctrine was taught at both the Infantry School and the Armor School as effective means to locate the enemy, move rapidly through a jungle environment, and surprise an enemy at night.

---

[59] Ibid., 8.

[60] Ibid.

[61] Ibid., 9.

During the 1970s doctrine reversed back to a focus on combined arms and its lethality and offensive capabilities. The October 1973 Middle East War, illustrated how lethal modern weapons had become. It also confirmed the likelihood of future tank on tank warfare; and once again, it reinforced the need to focus on combined arms. This re-focus brought about new doctrine in the form of a new and improved Field Manual 100-5, *Operations*. The new field manual stated that the United States must above all else, prepare to win the first battle of the next war.[62] This was especially true considering the highly mobile Soviet Armor threat in Europe. During 1976, Field Manual 71-100, *Armored and Mechanized Division Operations*, for example, repeated a theme frequently emphasized in Army manuals: "Envelopment is usually the preferred form of maneuver. Attacks are aimed at weak points in the enemy defense. If no weak point can be found, then one must be created."[63] The increased lethality of the tank made it the perfect piece of equipment to exploit or create a weak point. Doctrine was again adjusted to refocus Army leaders on the shock and awe capability of the tank. Additionally, doctrine also suggested that the larger reserve forces be moved forward so that their fire power could be used immediately against the enemy.[64] The most recent doctrine, U.S. Army Doctrine 2015, places equal emphasis on combined arms maneuver and wide area security. General (Retired) Gordon R. Sullivan wrote, "Without a solid intellectual foundation upon which to rest training, education, leader development, equipment modernization, and organizational design, the Army could easily have become disoriented and

[62] Doughty, 41.

[63] Ibid., 45.

[64] Ibid., 47.

unprepared."[65] Doctrine may change frequently and when it does, education and leader development must change with it. In the example of U.S. Armor above, its tactical doctrine changed repeatedly and as a function of that change, so did how the Army educated its leaders in the application of the tank. Like the tank, Army Aviation's doctrine and education followed a similar path of change during the period of 1946-1976.

The history of Army Aviation spans from the early 1900s to the present. In respect to Army Aviation, this thesis will include both the traditional fixed-wing and rotary-wing aviation. The reader should understand that the Army's traditional fixed-wing aviation eventually led to the formation of the U.S. Air Force. The introduction of both fixed-wing and rotary-wing aircraft changed how the Army developed leaders within the Aviation branch. This thesis will explore both fixed-wing and rotary-wing aviation only as far as they apply to the Army. The reader must understand that any Army Aviation platforms discussed after September 18, 1947 are considered rotary-wing aircraft only. The following key events, should illustrate how the Aviation branch changed over time and why it was necessary to make changes to doctrine and changes to Aviation leader development. On August 2, 1909, the Army took possession of its first airplane from the Wright Brothers.[66] On October 26, 1909 Army pilots made their first test flights.[67] On July 18, 1914, Congress created the first Air Section within the Signal

---

[65] General (Retired) Gordon R. Sullivan, quoted in General Raymond T. Odierno, Cover letter, Army Doctrine 2015 publications, September 5, 2012.

[66] Army Aviation, "Army Aviation Timeline," U.S. Army, accessed March 1, 2015, http://www.army.mil/aviation/timeline/index.html.

[67] Ibid.

Corps.[68] In 1916, General John Pershing used Army Aviation tactically for the first time to scout for Pancho Villa's raiders.[69] The Army created the Army Air Service in May of 1918.[70] Throughout the 1920s, the Army Air Service tested airplanes in bombing roles.[71] On July 1, 1926 Congress changed the Army Air Service to the Army Air Corps and created a Secretary of War for Air to manage the Corps.[72] In January of 1938, the Army Air Corps began to research and develop rotary-wing aircraft with an initial budget of two million dollars.[73] On November 1, 1941, the Army acquired its first helicopter, the Sikorsky YR-4.[74] On June 6, 1942 the War Department created organic Army Aviation under direction of Field Artillery and Army Ground Forces.[75] On September 18, 1947 the U.S. Air Force began operating separately from the Army.[76] On November 1, 1954 the Aviation School was moved from Fort Sill, Oklahoma to Fort Rucker, Alabama.[77] In early 1956, the Army began testing armament systems for helicopters.[78] In 1965, the First

---

[68] Ibid.

[69] Ibid.

[70] Ibid.

[71] Ibid.

[72] Ibid.

[73] Ibid.

[74] Ibid.

[75] Ibid.

[76] Ibid.

[77] Ibid.

[78] Ibid.

Cavalry Division validated the use helicopters in the Vietnam War.[79] On April 1, 1979 the Army received its first Black Hawk UH-60 helicopter.[80] On April 12, 1983, the Secretary of the Army approved Aviation to become the Army's 15th basic branch.[81] Today's Army Aviation platforms include the Apache AH-64, Kiowa Warrior, Black Hawk UH-60, Little Bird AH-6, and the Chinook UH-47 helicopters.[82] Army Aviation supports ground forces by providing lift, reconnaissance, fire support, security, medical evacuation, and close combat attack capabilities.

One of the main lessons the United States learned from combat operations during World War II was the need for closely coordinated and effective fire power.[83] From the battle grounds of Europe to Africa to the Pacific, all methods of coordinating and controlling close air support differed extensively.[84] Following World War II, "General Jacob L. Devers, chief of Army ground forces, stressed the integration of all available fire support means." [85] FM 31-35, Air Ground Operations, was published in August 1946. Unfortunately, inter-service rivalries stunted the development of Army Aviation doctrine during the late 1940s. Some Army leaders felt that helicopters could and should only be used for supporting airborne troop operations and ship-to-shore operations while others

---

[79] Army Aviation, "Army Aviation Timeline."

[80] Ibid.

[81] Ibid.

[82] Ibid.

[83] Doughty, 3.

[84] Ibid.

[85] Ibid.

believed they could be used for supply, evacuation, reconnaissance, observation, photography, column control, wire laying, and courier and liaison roles.[86] The Marines Corps rapidly integrated the helicopter into its doctrine and used it in combat operations in the early 1950s. The U.S. Army approached the integration of the helicopter into its doctrine a little more slowly. The largest change to doctrine during the early 1960s was the emphasis on vertical envelopments.[87] The Army's focus, in the 1960s, turned to counter insurgency and guerilla operations. In Vietnam, the U.S. Army felt the helicopter was the answer to the guerilla soldiers' speed. Brigadier General Carl L. Hutton made some significant additions and improvements to Army Aviation doctrine at the U.S. Army Aviation School at Fort Rucker, Alabama.[88] His emphasis on air transport and support of ground combat troops transformed curriculum at the Fort Rucker Aviation School. Early successes with the helicopter in 1961 caused Secretary of Defense Robert S. McNamara to recommend the helicopter be used even more extensively. This led to the formation and testing of an armed helicopter company in late 1962 into 1963.[89] The Armor and Aviation Schools both integrated courses designed to educate officers on the other branches' capabilities, tactics, techniques, and procedures. Additionally, advances in radio technology made commanding and controlling multiple different, dispersed units

---

[86] Doughty, 4.

[87] Doughty, 22; Headquarters, Department of the Army, Field Manual 1-02, *Operational Terms and Graphics* (Washington, DC: Government Printing Office, February 2015), 90. FM 1-02 defines vertical envelopment as a tactical maneuver in which troops, either air-dropped or air-landed, attack the rear and flanks of a force, in effect cutting off or encircling the force.

[88] Doughty, 27.

[89] Ibid., 29.

easier than before. Coordinating close air support, reconnaissance tasks, aviation technological capabilities, and command and control were now emphasized in branch specific schools (see tables 1 through 6). For more Armor and Aviation Program of Instruction details, see Appendices A through D.

It is important to note that the successful use of combined arms during World War II was a function of the introduction of the wireless radio to command and control systems. Heinz Guderian, a German "wireless officer,"[90] "responsible for developing the concept of Blitzkrieg, or fast moving mechanized warfare,"[91] was instrumental in the Blitzkrieg's initial successes because of his use of wireless radios during successful Panzer advances into Europe, Africa, and Russia.[92] The use of radios in tanks allowed units to move further and faster, coordinate direct and indirect fires, and maintain better situational awareness. This point is important because, in the same manner, the application of cyber digital communications to Command and Control systems underpins our current combined arms methods.

Tables 1, 2, and 3 illustrate how the Armor branch integrated curriculum focused on combined arms in order to ensure its officers were as well rounded and prepared to operate in complex and uncertain future as they could be. Tables 4, 5, and 6 illustrate how the Aviation branch did the same thing. Additionally, both branches increased the amount of combined arms curriculum over time. The curriculum listed in table 12 is

---

[90] Wireless officer is a term used to describe the German Signal branch of World War I.

[91] Your Dictionary, "Heinz Guderian Facts," LoveToKnow Corp., accessed April 27, 2015, http://biography.yourdictionary.com/heinz-guderian.

[92] Ibid.

clearly combined arms related curriculum. The curriculum listed in tables 13 and 14 may not initially appear to be combined arms related. The Aviation branch lists the purpose of Military Arts as providing "the student with a working knowledge of strategy, intelligence, operations, combined arms, and special subjects."[93] Army Aviation Employment curriculum provides "specific knowledge that will enable the student to employ various types of aviation assets including cargo, utility, operations and observation operations, and attack helicopter operations."[94] Aviator Review curriculum requires the student to understand a "general knowledge of communications, aviation medicine, roles of allied services, and command and control."[95]

[93] Norman E. Powell, Assistant Adjutant General, Memorandum, Subj: Program Change Proposal to Support Establishment of Aviation Officers Basic and Advanced Courses at the Aviation Center, Headquarters, U.S. Army Aviation Center, Fort Rucker, AL, January 10, 1979, 15.

[94] Ibid., 16.

[95] Ibid., 15.

Table 1. Curriculum and Hours, Program of Instruction, Armor Officer Basic Course, July 6, 1956

Armor Officer Basic Course	
Curriculum	Hours
Army Aviation Air Operations	2
Artillery Air Ground Operations	7
Engineering Operations	17
Infantry Operations	7

Source: The Armor School, *Program of Instruction for 17-0-A The Armor Officers Basic Course* (Fort Knox, KY: The United States Army Armor School, July 1956), 4-5.

Table 2. Curriculum and Hours, Program of Instruction, Armor Officer Career Course, August 10, 1961

Armor Officer Career Course	
Curriculum	Hours
Army Aviation Air Operations	15
Artillery Air Ground Operations	25
Engineering Operations	19
Tank and Mechanized Infantry Tactics	274

Source: The Armor School, *Program of Instruction for 17-A-C22 Armor Officer Career Course* (Fort Knox, KY: The United States Army Armor School, August 1961), 3.

Table 3. Curriculum and Hours, Program of Instruction, Armor Officer Advanced Career Course, August 10, 1961

Armor Officer Advanced Course	
Curriculum	Hours
Army Aviation Air Operations	19
Artillery Air Ground Operations	38
Engineering Operations	19
Tank and Mechanized Infantry Tactics	67

Source: The Armor School, *Program of Instruction for 17-0-3 The Armor Officer Advanced Course* (Fort Knox, KY: The United States Army Armor School, September 1956), 3-5.

Table 4. Aviation Basic Course Curriculum and Hours, per Program Change Proposal, January 10, 1979

Aviation Basic Course	
Curriculum	Hours
Combined Arms Operations	84
General Aviation Subjects	35
Maintenance and Supply	56
Common Military Tasks	91

Source: Norman E. Powell, Assistant Adjutant General, Memorandum, Subj: Program Change Proposal to Support Establishment of Aviation Officers Basic and Advanced Courses at the Aviation Center, Headquarters, U.S. Army Aviation Center, Fort Rucker, AL, January 10, 1979, 9.

Table 5. Aviation Advanced Course Curriculum and Hours, per Program Change Proposal, January 10, 1979

Aviation Advanced Course	
Curriculum	Hours
Military Arts	203
Army Aviation Employment	87
Simulated Aviation FTX	35
Aviator Review	175

Source: Norman E. Powell, Assistant Adjutant General, Memorandum, Subj: Program Change Proposal to Support Establishment of Aviation Officers Basic and Advanced Courses at the Aviation Center, Headquarters, U.S. Army Aviation Center, Fort Rucker, AL, January 10, 1979, 13.

Table 6. Aviation (CORE) Advanced Course Curriculum and Hours, per Program Change Proposal, January 10, 1979

Aviation (CORE) Advanced Course	
Curriculum	Hours
Aviation Review	123
Army Aviation Employment	90
Simulated Aviation FTX	35

Source: Norman E. Powell, Assistant Adjutant General, Memorandum, Subj: Program Change Proposal to Support Establishment of Aviation Officers Basic and Advanced Courses at the Aviation Center, Headquarters, U.S. Army Aviation Center, Fort Rucker, AL, January 10, 1979, 17.

Curriculum within Army learning institutions like Infantry Officer's Basic Course, Officer Candidate School, and Intermediate Level Education at the Command and General Staff College teach the importance of combined arms. The following sections will discuss specific Army learning institutions, their missions, and curriculum related to combined arms and the lack of cyber education as part of that combined arms curriculum.

The Infantry Basic Officer's Leadership Course's mission is to educate, train, and inspire Infantry lieutenants so that upon graduation, they demonstrate the competence, confidence, physical and mental toughness, and moral/ethical fiber necessary to lead platoons in any operational environment.[96] This seventeen-week course prepares Infantry lieutenants to lead platoons by providing them with basic instruction on tactics, techniques, leadership, writing, and physical fitness. There is no mention of cyberspace instruction anywhere in the curriculum. Figure 15 provides an overview of the seventeen-week Infantry Basic Officer's Leadership Course. Weeks twelve, thirteen, and fourteen focus on combined arms exercises. Week twelve features an urban field training exercise, followed by a shoot house live fire exercise, followed by another urban field training exercise. The incorporation of armor, aviation, and indirect fires assets is taught during classroom portions and practiced during the field training exercises.

[96] U.S. Army Maneuver Center of Excellence, "IBOLC Mission," U.S. Army, December 10, 2014, accessed December 23, 2014, http://www.benning.army.mil/infantry/199th/ibolc/content/pdf/IBOLC_Mission_Statement.pdf.

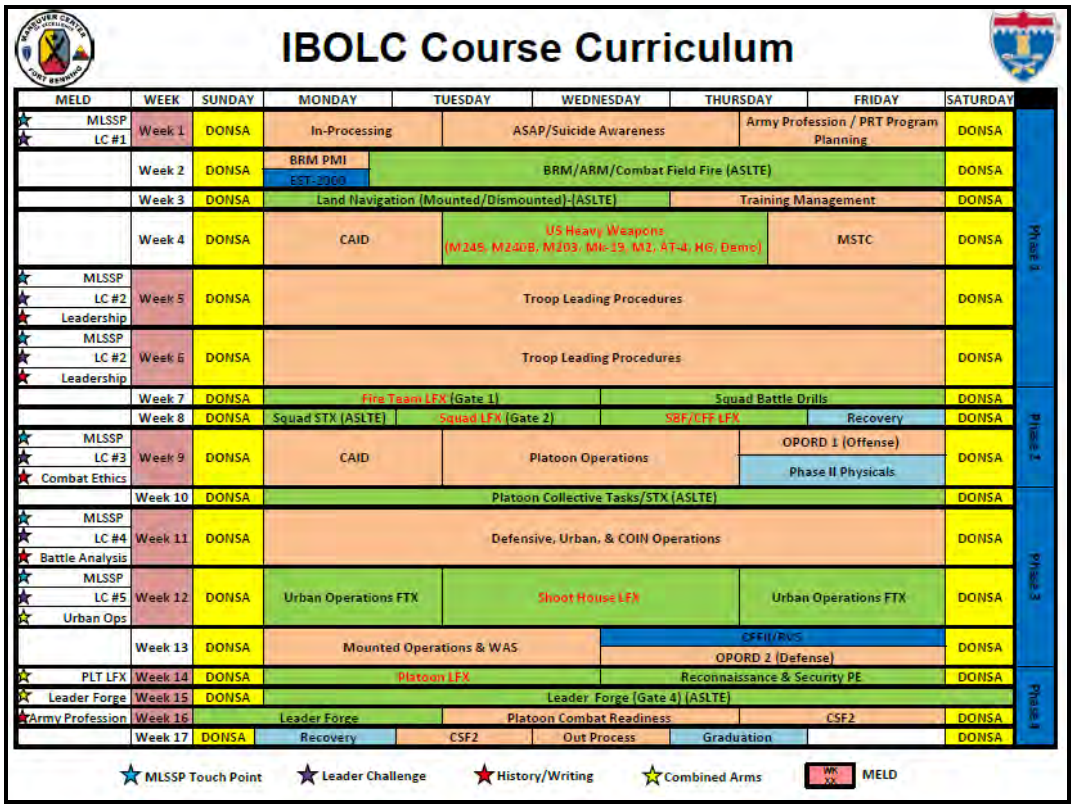


Figure 9. Seventeen-week Infantry Basic Officer's Leadership Course Curriculum Overview

Source: U.S. Army Maneuver Center of Excellence, "IBOLC Course Curriculum," U.S. Army, accessed January 24, 2015, http://www.benning.army.mil/infantry/199th/ibolc/.

The U.S. Army Officer Candidate School, located at Fort Benning, Georgia "provides trained, agile, and adaptive junior officers for an Army at war who are ready today and relevant for tomorrow's challenges."[97] The twelve-week course offers curriculum ranging from leadership, ethics, and military intelligence to training management, tactics, and military history. They do not however, offer any curriculum

[97] U.S. Army Maneuver Center of Excellence, "Officer Candidate School (OCS)," U.S. Army, March 6, 2015, accessed April 9, 2015, http://www.benning.army.mil/infantry/199th/ocs/.

that includes cyberspace. Additionally, the Officer Candidate School conducts a Field Leadership Exercise that allows the candidates to apply combined arms course curriculum. See Appendix E, Officer Candidate School Twelve-week Training Plan.

The Command and General Staff College integrated cyberspace into its curriculum in approximately 2012. A two-hour cyberspace module is now embedded inside the common core C300 courses. The objective of C310, Cyberspace Operations is to provide an understanding of the "fundamentals of cyberspace operations through preparatory readings followed by classroom discussion and in-class exercises. Upon completion of this lesson, you will comprehend cyber functions, capabilities and limitations; and how cyber operations are integrated in joint planning for unified action."[98] The module also affords the student the ability to "comprehend and use the fundamentals of cyberspace operations related to unified action, joint force organizations, joint command authorities; and the relations between the Combatant Commands (CCMDs), Strategic Command (STRATCOM) and its sub-unified command Cyber Command (CYBERCOM)."[99] See Appendix F for more detailed information on C310, Cyberspace Operations Module. Cyberspace is also reinforced in the C206 lesson, Theater Assessments and Strategic Estimates. The C206 joint professional military education learning area reinforces comprehension of "the role and perspective of the combatant commander and staff in developing various theater policies, strategies, and

---

[98] U.S. Army Command and General Staff College, "C300 Lessons," Blackboard, accessed December 22, 2014, https://cgsc.blackboard.com/webapps/portal/frameset.jsp?tab_tab_group_id=_2_1&url=/webapps/blackboard/execute/launcher?type=Course&id=_3204_1&url=.

[99] Ibid.

plans, to include weapons of mass destruction/effects (WMD/E); IO; cyberspace operations; Stability, Security, Transition and Reconstruction (SSTR); intelligence; logistics; and strategic communication."[100] The Command and General Staff College also enables students to notionally include cyberspace into their planning during the end of common core Joint Operations Planning Process exercise.

The Command and General Staff College allows students to utilize their experience and choose electives following the Advanced Operations Phase of the course. For the purpose of this thesis, the individual student's choice qualifies this as falling within the self-development domain of leader development because the student chose electives based on personal interests rather than a set curriculum. The Command and General Staff Officers Course Electives Program Memorandum of Instruction for Class AY2015 lists three electives that address cyberspace. A564, Foundations of Cyberspace Operations, provides a "foundation for field grade officers to competently operate in an increasingly cyber reliant environment."[101] A338, Advanced Intelligence Seminar is a discussion based class that includes the topic of cyber warfare as it relates to the intelligence warfighting function.[102] The final cyber related elective the Command and General Staff College offers is A532, Joint Targeting. This elective explores computer

---

[100] U.S. Army Command and General Staff College, "C206 Theater Assessments and Strategic Estimates," Blackboard, accessed December 22, 2014, https://cgsc.blackboard.com/webapps/portal/frameset.jsp?tab_tab_group_id=_2_1&url=/webapps/blackboard/execute/launcher?type=Course&id=_3096_1&url=.

[101] Marvin L. Nickels, Subject: Command and General Staff Oficers Course (CGSOC) Electives Program Memorandum of Implementation (MOI) for AY2015, U.S. Army Command and General Staff College, Fort Leavenworth, KS, December 8, 2014, AY15 Enclosure-3, 249-250.

[102] Ibid., 58.

network and cyber warfare operations.[103] Each elective provides the student with approximately twenty-four hours of course study or contact time with an instructor. The Command and General Staff College has also entered into an agreement called Outreach to Department of Defense with Kansas State University. The purpose of the agreement is to "develop a comprehensive cybersecurity curriculum which addresses the challenge of educating and providing hands-on training to students of broad academic backgrounds."[104] Additionally it provides "innovative modules and lesson plans based on lab exercises, warfare and cyber-threat scenarios which can seamlessly integrate security education throughout different parts of students' existing information technology curriculum."[105] This agreement provides students at the Command and General Staff College four additional electives. Elective one, Introduction to information assurance and cybersecurity is available during the Command and General Staff College's common core phase. Elective two, Emerging Threats in cyberspace is available during the Command and General Staff College's advanced operations phase. Elective three and four are both offered during the Command and General Staff College's electives phase. They are titled Advanced Cyber-offense and defense Technologies and Cyber warfare respectively.[106] See Appendix G for more detailed information regarding the Outreach to Department of Defense Agreement.

---

[103] Nickels, 208-209.

[104] Kansas State University, "DoD Information Assurance Scholarship Program," Annex II-Capacity Building, Technical Proposal-Project Name: Outreach to Department of Defense, Kansas State University, Manhattan, KS, 2011, 1-5.

[105] Ibid.

[106] Kansas State University, "DoD Information Assurance Scholarship Program."

The mission of the School of Advanced Military Studies is to "educate students at the graduate level to become agile and adaptive leaders who are critical and creative thinkers who produce viable options to solve operational and strategic problems."[107] The eleven-month course offers three cyber lessons, an engagement with ARCYBER points of contact, and an opportunity to attend an ARCYBER Executive Cyberspace Operations Planners Seminar. The first cyber lesson is taught in the Morality and War Course and discusses the ethics of cyber warfare. The second cyber lesson is taught in the Contemporary Operational Art Course and focuses on the space and cyber domains. In this lesson, students are assigned eleven cyber and space related readings in order to prepare for the space and cyber discussion. The third lesson is taught during the Cyber II block and focuses on social media. Reference Appendix H for the learning objectives.

The battalion and brigade level Pre-Command Courses offer minimal cyberspace course hours. The extent of the Pre-Command Course's cyber curriculum is a lecture from the commander of the Army's Cyber Command. This lecture is classified Secret. During phase three of the pre-command course, the soon to be commanders travel to their specific centers of excellence and receive more in depth training and education related to their functional areas. Example—infantry and armor leaders travel to Fort Benning, Georgia and attend courses at the Maneuver Center of Excellence. Signal or cyber leaders will travel to Fort Gordon, Georgia to receive more specialized cyber and signal related courses.

---

[107] United States Army Combined Arms Center, "School of Advanced Military Studies (SAMS)," U.S. Army, February 25, 2015, accessed April 11, 2015, http://usacac.army.mil/organizations/lde/cgsc/sams.

Company grade signal leaders attending Signal Officers Basic Course and Signal Captain's Career Course receive more education on cyberspace than other branches discussed in this thesis. Signal Captain's Career Course students receive eighty hours of education focusing on Signal Common Core including Combat Net Radio, Army Battle Command Systems, and Warfighter Signal Support. The eighty hours of signal common core training leads up to a Digital Live Fire Range Capstone exercise "in which students manage full blown WIN-T architecture through actual equipment for five full days in real time with support from staff members from General Dynamics.[108] General Dynamics staff are able to introduce injects including cyber-attacks and then evaluate student performance in dealing with the attack. "The intent for Signal captains is to recognize specific problems, like cyber-attacks, identify its cause, raise the issue appropriately, and – most importantly – brief their chain of command on the potential operational impact on the mission at hand."[109] Additionally, Signal Captain's Career Course leaders have expanded on the cyberspace education their students receive by bringing in 2nd Information Operations Battalion world-class cyber opposing force personnel to help signal captains focus on basic information assurance operations and detecting, reporting, and mitigating cyber threats.[110]

The Army has implemented a cyber-awareness program across the regular Army. Every time a DOD Employee accesses a government computer, the computer will present

---

[108] Captain Kristen M. Johnson, "Remaking the Signal Captain - A New Training Equation For Success," *Army Communicator* 38, no. 1 (Spring 2013): 21.

[109] Ibid., 22.

[110] Ibid., 23.

the operator with three different screens. The first screen informs the operator of an Army Cyber Alert and to Always Practice Good Cyber-security. This screen also tells the operator to save the government money by turning off unused equipment if it is to be left unattended for longer than thirty minutes (see figure 16). After approximately five seconds, the government computer switches to another screen that lets the user know that they are the first line of defense for cyber-security (see figure 17). The first two screens always depict the same alert and warning. The third and final screen poses an information assurance cyber-awareness question of the day. The screen prompts the user to answer the question. If the user answers the question correctly, the screen will provide a response highlighted in green stating that the user has answered the question correctly. An incorrect response triggers a red highlighted response stating You Answered Incorrectly (see figure 18). Regardless of the response, the user is then allowed access to the government system. The information assurance question of the day screen varies and poses different questions every time a user accesses the computer. The questions generally force the user to choose between two different answers. Of note, the user has the option to not answer the question and just X out of the information assurance question of the day screen and go directly to the desk top.

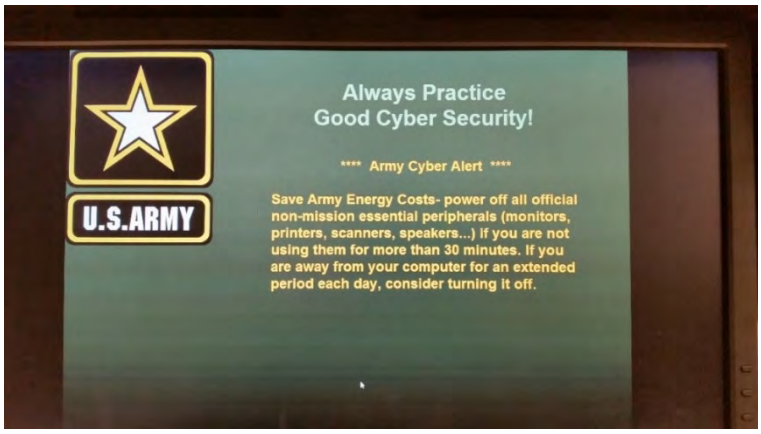


Figure 10. Army Cyber Alert Screen

Source: Photo by author of DOD computer screen, initial Cyber Alert message, Fort Leavenworth, KS, February 2, 2015.

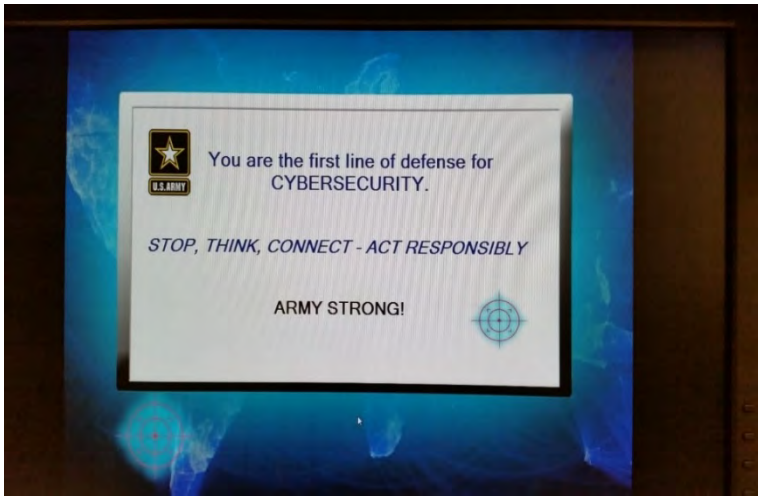


Figure 11. Army CYERSECURITY Message

Source: Photo by author of DOD computer screen, second cyber message screen, CYBERSECURITY, Fort Leavenworth, KS, February 2, 2015.

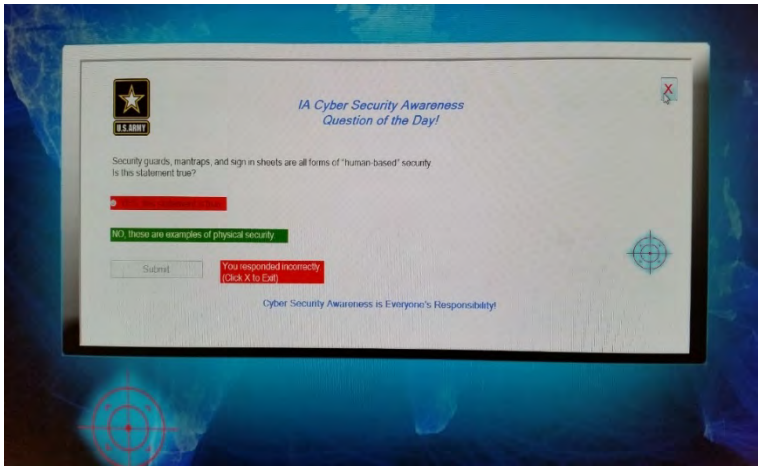


Figure 12. Information Assurance Cyber Security Awareness Question of the Day

Source: Photo by author of DOD computer screen, third cyber message screen, IA Cyber Security Awareness Question of the Day!, Fort Leavenworth, KS, February 2, 2015.

In short, Army learning institutions including the Officer Candidate School, the Infantry Officer Basic Course, the Command and General Staff College's Intermediate Level Education, the School of Advanced Military Studies, and the Pre-Command Courses include very little cyberspace curriculum. The Officer Candidate School and the Infantry Officer Basic Course do not offer any cyberspace curriculum. The Command and General Staff College's Intermediate Level Education offers students two hours of cyber common core, an opportunity to take a number of cyberspace related electives, and an opportunity to take cyber related courses at Kansas State University through an Outreach to Department of Defense program. Of all the TRADOC leader development courses, only the Signal Captain's Career Course includes a significant amount of cyberspace curriculum.

This chapter provided the background information the reader needed to understand how and why the Armor and Aviation branches were formed and what changes were made to Army doctrine to compensate for the emergence of the tank and the helicopter. Second, this chapter discussed the development of the Armor and Aviation schools specifically created to develop the leaders within those branches. Third, this chapter provided details on the curriculum from some of the Army's learning institutions in order to determine if the Army has programmatically included cyberspace into the institutional domain's education pillar of leader development as effectively as it could be. The research conducted allows the author to answer the primary and secondary research questions proposed in chapter 1.

The primary research question was: Is TRADOC programmatically integrating cyberspace into the leader development domains as effectively as it should? The cross case comparative analysis showed that the Armor branch integrated aviation curriculum into its branch specific school. The analysis also showed that the Aviation branch integrated armor curriculum into its branch specific schools. Furthermore, both branches acknowledged the importance of combined arms and integrated curriculum from every other branch into their specific schools in amounts that far outweigh the cyberspace curriculum the Army currently offers its non-cyber branched officers. This information led the author to conclude that TRADOC is not programmatically integrating cyberspace into the leader development domains as effectively as it could. Chapter 5 will explain in more detail why the author drew this conclusion, the caveats associated with this conclusion, and provide the reader the answers to the three secondary research questions of this thesis.

CHAPTER 5

CONCLUSION AND RECOMMENDATIONS

Although Cyberspace provides tremendous opportunities, it also provokes even larger potential threats. The President of the United States, Secretary of Defense, and Chairman of the Joint Chiefs of Staff, have made cyberspace, and its defense, a priority. They have done so by addressing it in the *National Defense Strategy*, the *Quadrennial Defense Review,* and the *National Military* Strategy of the United States of America. However, the U.S. Army Chief of Staff's number one priority is leader development. These two priorities come together in the schoolhouse where instruction on cyberspace can impact leader development. The author conducted this research because there was a perceived gap between the importance of cyberspace and the amount of cyber education officers were receiving during their sojourns to key leader development billets like the Officer Candidate School, the Infantry Officer Basic Course, the Army's Intermediate Level Education at the Command and General Staff College, the School of Advanced Military Studies, and the Pre-Command Courses. The author did not feel the U.S. Army was placing the appropriate emphasis on developing cyber savvy leaders within the institutional domain's education pillar.

Chapter 5 will provide the reader with a brief summary of the findings from chapter 4. The author will interpret the findings described in chapter 4 and explain what the results mean, what the implications are, and list any unexpected findings. The author will also make recommendations for further study and recommendations for action.

The cross case comparative analysis examined the Armor and Aviation branches and the curriculum their branch specific schools offered to officers and then compared it

to present day cyber curriculum offered in Army learning institutions like the Officer Candidate School, the Infantry Officer Basic Course, Intermediate Level Education at the Army's Command and General Staff College, the School for Advanced Military Studies, and the Pre-Command Courses.

The tank was first introduced in World War I, the Tank Service was formed on March 5, 1915, the U.S. Armor School was established in October of 1940, and Armor officially became a branch in 1950. From the introduction of the tank, it took the Army approximately twenty years to create a school specifically designed to educate leaders on armor. It took thirty years from the introduction of the tank before the Army created the official Armor branch. The Armor school at Fort Knox, Kentucky developed and taught curriculum that ensured its leaders were educated on the doctrine and tactics of other branches such as Infantry, Field Artillery, Army Aviation, and Engineering. The Army of 1950 spent more hours teaching combined arms curriculum to its officers than the Army of today does with cyberspace education.

The Army Air Service was created in May of 1918. From 1918 to 1941 the Army used fixed-wing aircraft. The Army secured its first helicopter in November 1941 and was designated an organic branch under the Field Artillery Corps. In 1954 the Aviation School moved from Fort Sill, Oklahoma to Fort Rucker, Alabama. The First Cavalry Division extensively tested and validated the use of helicopters in combat during the Vietnam War. Following the Vietnam War, the Army conducted extensive studies between 1970 and 1982 on the future of the helicopter and its role in the Army. Army Aviation became an official branch on April 12, 1983 and Aviation Basic and Advanced Courses began in early 1984. From the introduction of the helicopter, it took

approximately forty years to create an Aviation Officers' Basic and Advanced Course. It took approximately forty-two years for the Army to make Aviation an official basic branch. The curriculum taught in the Aviation School's Basic and Advanced Courses clearly illustrates the emphasis placed on educating its officers on the doctrine and tactics of other branches to include Infantry, Armor, and Field Artillery. Similar to the Armor branch in the 1950s, the number of Infantry, Armor, and Field Artillery curriculum hours taught at the Aviation school in the 1980s is significantly greater than what current Army learning institutions are spending on educating officers on cyberspace. Just like the Armor branch of the 1950s, the aviation branch offered combined arms curriculum to its officers in the inaugural Basic, Career, and Advanced Courses. The fact that both the Armor and Aviation branches offered combined arms curriculum from the start of their leader development courses belies the importance of educating our junior and mid-grade officers on combined arms. As mentioned in chapter 4, combined arms as it is currently known is a function of the introduction of the radio to command and control systems. In the same manner, the application of cyber digital communications systems underlies the way the Army applies today's version of combined arms. Cyberspace is the medium through which the U.S. Army applies Command, Control, Computers, Communications, Intelligence, Surveillance, and Reconnaissance. Cyberspace is also the underlying function for targeting and navigation. It would be difficult for the U.S. Army to effectively fight a combined arms battle without the use of cyberspace. Cyber related systems have replaced all the old analog methods the U.S. Army originally used to command and control combined arms forces.

The Army switched on its first computer in 1946. It was called the Electronic Numerical Integrator and Computer. It was digital, could be re-programmed, and was able to solve a wide variety of numerical problems.[111] The Internet was first created in 1969 as a node to node communication system.[112] Both the Electronic Numerical Integrator and Computer and the early version of the internet were extremely limited in their capabilities and should not be used as the beginning of modern cyberspace's timeframe. However, it can be argued that the AN/GSG -10 TACFIRE system, the pre-cursor to the Advanced Field Artillery Tactical Data System, is the real start to the Army's use of digital/cyber systems in the field. The last fielding for the TACFIRE system occurred in the late 1980s and was replaced by the Advanced Field Artillery Tactical Data System in the mid 1990s.[113] The Army's Chief of Staff, General Raymond Odierno and the Secretary of the Army, John McHugh approved the activation of the

[111] Egon Hatfield, "Women's History Month: ENIAC, first computer programmers," U.S. Army, March 18, 2013, accessed April 11, 2015, http://www.army.mil/article/98817/Women_s_History_Month__ENIAC__first_computer_programmers/.

[112] Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff, "Brief History of the Internet," Internet Society, accessed April 11, 2015, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet. "The Electronic Numerical Integrator and Computer" and the earliest known version of the internet serve only as points of reference for the reader to better understand when the technologies were first introduced; not as the beginning of what this thesis defined as cyberspace.

[113] Elizabeth A. Stanley, *Evolutionary Technology in the Current Revolution in Military Affairs: The Army's Tactical Command and Control System* (Darby, PA: Dianne Publishing Company, 1998), 29.

Army Cyber branch in September of 2014.[114] In April 2015 the Army opened the U.S. Army Cyber School at Fort Gordon, Georgia.[115] The first Cyber Basic Officer Leaders Course will commence the summer of 2015.[116]

The 1990s brought on the widespread introduction of the desktop computer into unit training rooms all across the Army and also witnessed the growing use of the Internet in the late 1990s. From the fielding of the initial Advanced Field Artillery Tactical Data System and the widespread introduction of the desk top computer in unit training rooms in the mid 1990s, it took the Army approximately twenty years to make Cyber an official basic branch and create a branch specific school that would educate leaders on cyberspace. The number of cyberspace curriculum hours taught in Army learning institutions, other than the U.S. Army's Cyber School, is significantly less than what other branch specific schools taught when there was a technological advancement like the introduction of the tank and the helicopter. With respect to organization, the Army's response to cyberspace as a technology requiring its own branch is generally within the same timeframe as was the case with the tank and helicopter.

Lieutenant General Cardon's belief that anything that can pass a "1 and 0" can be used as a weapon,[117] combined with the fact that the Army created the Cyber branch to develop leaders that can operate in and through cyberspace, illustrates the point that

---

[114] George I. Seffers, "U.S. Army Builds Cyber Branch One Step at a Time," *Signal* (April 1, 2015), accessed April 11, 2015, http://www.afcea.org/content/?q= Article-us-army-builds-cyber-branch-one-step-time.

[115] Ibid.

[116] Ibid.

[117] Cardon.

cyberspace is now one of the military's combined arms. As such, the Army should better integrate cyber curriculum into the leader development's institutional domain. TRADOC should follow the examples set by the Aviation and Armor branches and their integration of combined arms curriculum into their courses.

The bottom line is that the Armor and Aviation branches were including more combined arms curriculum focused on integrating other branches at this point in their development than the Army is currently doing with cyberspace in today's Army learning institutions. Unlike the Armor and Aviation branches at this stage of their development, Army learning institutions are not integrating cyberspace into current combined arms curriculum and this is why the author has concluded that the Army is not programmatically integrating cyberspace into leader development as well as it should. The Army did a better job of integrating the tank and helicopter into its combined arms curriculum.

In chapter 1 of this thesis, the author made the assumption that the Army's Leader Development Strategy was not broken. After conducting this research, that assumption still holds true. The author hypothesized that the Army was not programmatically integrating cyberspace into leader development as well as it should. The null hypothesis is that the Army is programmatically integrating cyberspace into leader development as well as it could. The research led the author to conclude that the Army is not integrating cyberspace into leader development as effectively as it could and to reject the null hypothesis.

"Army Cyber conducted a capabilities based assessment in 2010–2011 to determine the doctrine, organization, training, materiel, personnel and facilities gaps."[118] However, the leader development, education, and training aspects were not considered. The second capabilities based assessment conducted "confirmed the need for a thorough analysis of leadership, training, and education to better enable ARCYBER to develop an assessment and implementation strategy."[119] ARCYBER recently developed an assessment and implementation strategy that identifies how cyberspace will be integrated into leader development process, who falls into the category of requiring cyber education and what cyber subject matter is unique to that specific population, and at what time in an officer's career to introduce specific cyber subject matter. See Appendix I for the section three extract from the "Leader Development, Education, and Training Assessment and Implementation Strategy." The author's conclusion does not mean that the Army has not examined cyberspace and its role in the Army. In fact, the Army has integrated cyberspace curriculum into four Army learning institutions—the Signal Captain's Career Course, the Command and General Staff College's Intermediate Level Education, the School of Advanced Military Studies and, in a more limited capacity, the Battalion and Brigade level Pre-Command Courses.

Army Cyber's Assessment and Implementation Strategy identifies the population that should receive cyber education and what that education should comprise. ARCYBER

---

[118] Army Cyber Command, Force Modernization Proponent, "Army Cyberspace Leader Development, Education And Training (LDE & T) Assessment and Implementation Strategy," Army Cyber Command, Leavenworth Support Element, July 1, 2013, 4.

[119] Ibid., 5.

believes that basic cyber awareness is all that is needed at the Soldier and junior leader levels. Soldiers and junior leaders should be able to "identify a possible adversarial attack, perform initial actions, and report the incident."[120] "Leaders require additional cyber knowledge in order to mentor and develop subordinate Army leaders."[121] Staffs must have the cyber expertise to understand what effects the use of cyberspace will achieve and how it can be effectively integrated into all planning processes. Staffs must also have enough cyber knowledge to be able to inform the commander.[122] "Commanders need a baseline understanding of their unit's cyber related vulnerabilities as well as effects that can be leveraged against an adversary."[123] Unfortunately, if cyber curriculum is not integrated into courses like the Officer Candidate School, Officer Basic Courses, and Captain's Career Courses, junior leaders will not be able to identify a possible attack, perform initial actions, or report.[124] Intermediate Level Education does not offer more than two common core cyber curriculum hours and there is no formal cyber integration during the O199, O299, and O399 exercises. Soon to be staff officers, graduates of Intermediate Level Education, therefore are not receiving enough cyber expertise to

[120] Army Cyber Command, Force Modernization Proponent, "Army Cyberspace Leader Development, Education And Training (LDE & T) Assessment and Implementation Strategy," 12.

[121] Ibid.

[122] Ibid.

[123] Ibid.

[124] Ibid.

understand what effects the use of cyberspace will achieve nor how to effectively integrate it into the planning process.[125]

The research also enabled the author to answer the three secondary questions of this thesis. With respect to the first secondary research question: Should cyberspace be included in the institutional, operational, and self-development pillars of leader development? Yes, cyberspace should be included in the, institutional, operational, and self-development pillars of leader development because cyberspace is both an opportunity and a threat. This point is illustrated by the beliefs of our senior leaders and their strategic documents mentioned earlier in this thesis. In order for the Army to operate effectively within cyberspace, its leaders must be developed with cyberspace in mind. In regards to the second secondary research question: When should the U.S. Army begin to develop cyber savvy leaders? The U.S. Army should begin to develop cyber savvy leaders at the company grade level. If ARCYBER's assessment and implementation strategy is viable, junior officers attending courses Officer Basic Courses and Captain's Career Courses should receive cyber education so they can identify an adversarial cyber-attack, perform initial actions, and report to higher. Cyber education for junior officers is a critical component of executing the ARCYBER's assessment and implementation strategy. The third secondary research question: Do we allow one command, USCYBERCOM or ARCYBER, to develop our cyber savvy leaders? Although USCYBERCOM and ARCYBER are the main proponents for cyberspace, every command should make their responsibility to develop their own cyber savvy leaders; it

[125] Army Cyber Command, Force Modernization Proponent, "Army Cyberspace Leader Development, Education And Training (LDE & T) Assessment and Implementation Strategy," 12.

should not be the responsibility of one single command. If ARCYBER is singly responsible for developing cyber savvy leaders, and only a small percentage of the U.S. Army's officers will get an opportunity to attend ARCYBER's cyber school, the officer corps as a whole will not be as cyber savvy as they should be. The last point further illustrates the need to include cyberspace in the combined arms and supports the author's conclusion that cyberspace curriculum should be better integrated, at lower levels, into the Army's learning institutions.

Recommendations for Further Study

1. Is the Army Cyber School adequately preparing junior officers to integrate cyber operations into mission planning?
2. Is ARCYBER's Assessment and Implementation Strategy working?

Recommendations for Action

1. Lengthen Intermediate Level Education from ten months to eleven months to include more cyber curriculum. Specifically increase C310 Cyberspace from two hours to six hours and discuss the ethics of operationalizing cyberspace.
2. Include Cyber Operational planning into the Command and General Staff College's O100-O300 exercises.
3. Refine the Command and General Staff College's Intermediate Level Education current two-hour C310 curriculum to better meet the stated Enabling Learning and Terminal Learning Objectives then intergate into the Officer Basic and Captain's Career Courses.

4. Change the settings on the IA Cyber Security Awareness Question of the Day to not allow operators to X out of the screen and proceed directly to their desk tops. Additionally, change the software to ensure that operators must answer the questions correctly. If a question is answered incorrectly, force the operator to answer questions until they do answer correctly.
5. Develop software that tracks unit performance on the Information Assurance Cyber Security Awareness Questions of the Day so commanders can be provided an assessment of their unit's cyber awareness.

In conclusion, cyberspace is both an opportunity and a threat. Senior leaders from the President down to the Army's Cyber Command understand the importance of developing cyber savvy leaders. ARCYBER has developed an assessment and implementation strategy that has identified the Who, What, Where, When, and How of cyber integration into leader development. That implementation plan went into effect in Fiscal year 2014 and is just in its infancy. The amount of cyberspace curriculum in Army learning institutions has increased over the last three years but still does not match the number of curriculum hours the Armor and Aviation branches focused on combined arms curriculum at the same stage in their development. If the current amount of cyberspace curriculum remains the status quo, the implications will be disastrous for the Army. It will not be possible for the Army to defend itself against cyber-attacks; nor will it be able to effectively plan and integrate cyberspace into offensive and defensive operations.

APPENDIX A

ARMOR OFFICER BASIC COURSE PROGRAM OF INSTRUCTION

THE ARMOR SCHOOL

FORT KNOX, KENTUCKY

JUNE 1956

PROGRAM OF INSTRUCTION

FOR

17-0-A

ARMOR OFFICER BASIC COURSE

MOS: None

Length: Peacetime—16 weeks
Mobilization—13 weeks

APPROVED BY COMMANDING GENERAL, CONTINENTAL ARMY COMMAND
6 JULY 1956

SECTION I–PREFACE

A. Course: 17-O-A, Armor Officer Basic.

B. Purpose: To provide minimum essential branch training for newly commissioned Armor officers to enable them to perform the duties of a platoon leader in a tank or reconnaissance company. MOS for which trained: None.

C. Prerequisites: Newly commissioned second lieutenants from all sources other than Armor OCS whose assignment, actual or anticipated, is to Armor. Security clearance to include CONFIDENTIAL.

	Peacetime	Mobilization
D. Length:	16 weeks–704 hours	13 weeks–624 hours
E. Training Locations:	The Armor School	The Armor School
F. Percentage of Training Requirement to be School Trained:	100%	100%

G. MOS Feeder Patterns: Not applicable.

H. Ammunition Requirements: See section V.

I. Common Subjects Recapitulation: See section VI.

NOTE: Program of Instruction approved by 1st Indorsement, ATARM 352.11 (11 Jun 56) Continental Army Command, 6 July 1956, subject: "POI for Armor Officer Basic Course, 17-O-A" to letter AICBB-A 352.11 (11 Jun 56) The Armor School. The approved program of instruction was printed in accordance with instructions and format outlined in letter ATTNG-P&O 352.11/223(6 Aug 56), Hq, CONARC, dated 6 August 1956, subject, "Dual Programs of Instruction."

SECTION II–SUMMARY

ARMOR OFFICER BASIC COURSE

Length: Peace: 16 weeks–704 hours.
Mobilization: 13 weeks–624 hours.

Subject AOB		Hours Peace	Mob	Annex Nr	Page Nr
~~A. ACADEMIC SUBJECTS~~		FY57	FY58		
1–Automotive Department					
Automotive General		10 12	10	1A	10
Maintenance Administration and Inspection		9 10	9	1B	11
Driving and Driving Principles		14 14	14	1C	11
Preventive Maintenance Services		29 30	29	1D	12
Examination and Critique		4 4	4	1E	15
	Sub-Total	66 70	66		
2–Command and Staff Department					
Introduction		1 1	1	2A	15
Armor Employment		80 82	80	2B	15
(1) Team and Task Force; Combat Command and Division	58 60				
(2) Reconnaissance Operations	20 23				
(3) Army Aviation	2 2				
Air Operations		2 2	2	2C	20
Amphibious Operations		2 2	2	2D	20
Special Weapons		10 10	10	2E	21
Staff Subjects					
Intelligence		12 10	12	2F	22
Logistics and Personnel		9 9	9	2G	23
~~Operations~~ Staff Subjects		9 7	9	2H	24
Associate Arms					
Artillery, Air-Ground Operations System Fire-Support Coordination		7 7	7	2I	25
Infantry Operations		7 10	7	2J	26
Engineer Operations		17 15	17	2K	26
(1) Field Engineering	10 8				
(2) Mine Warfare	7 7				
Examinations and Critiques		10 10	10	2L	27
	Sub-Total	166 168	166		
3–Communication Department					
Communication Procedure		11	11	3A	28
Communication Equipment		18	18	3B	29
Tactical Communication		16	16	3C	31
Field Communication		19	19	3D	32
	Sub-Total	64 64	64		
4–General Subjects Department					
Physical Conditioning		27 14	12	4A	34
Drill and Ceremonies		17 19	0	4B	37
Civil Emergencies		4 0	4	4C	38
Company Administration + Supply + Food Service		9 10	2	4D	39
Military Leadership		10 8	8	4E	39
Military Topography		19 27	19	4F	40
Instructor Training		26 26	25	4G	41
MILITARY JUSTICE		0 4			
Command Inspection		8 8			
Training Management		0 8			

Subject	Hours Peace	Hours Mob	Annex Nr	Page Nr
Medical Subjects	4 3	4	4H	43
~~Supply and Food Service~~	~~5~~	4	4I	43
Reserve Components	1 0	0	4J	44
Code of Conduct	1 1	1	4K	44
Psychological Warfare	1 1	1	4L	45
Public Information and Community Relations	1 0	1	4M	45
Troop Information and Education	1 1	1	4N	46
The Army Position in National Defense	2 2	0	4O	46
Nonresident Instruction and Training Assistance	1 1	0	4P	46
Department Director's Orientation	1 1	1	4Q	47
Armor Military Stakes	4 4	4	4R	47
Tanker's Night Ride	8 8	8	4S	47
Examination and Critique	8 8	8	4T	48
Sub-Total	~~145~~ 153 154	103		
5–Weapons Department				
Small Arms	68 66	68	5A	48
Materiel	30 34	30	5B	51
Tank Gunnery	89 87	89	5C	51
Sub-Total	187 187	187		
B. NONACADEMIC SUBJECTS				
Commandant's Time	32 32	26	Omitted	
Open Time	8 ~~16~~ 9	0	Omitted	
In-Processing	20 12	8	Omitted	
Out-Processing	8 8	4	Omitted	
Sub-Total	68 ~~76~~ 61	38		
Total	704	624		
C. RECAPITULATION				
1. Security Classification:				
CONFIDENTIAL	13	13		
UNCLASSIFIED	691	611		
Total	704	624		
2. Type of Instruction				
Conference	201	191		
Demonstration	60	50		
Practical Exercise	332	310		
Examination	35	35		
Nonacademic Subjects	76	38		
Total	704	624		

62

13 4/5

APPENDIX B

ARMOR OFFICER CAREER COURSE PROGRAM OF INSTRUCTION

US ARMY ARMOR SCHOOL
FORT KNOX, KENTUCKY

SEPTEMBER 1962

PROGRAM OF INSTRUCTION

FOR

17-A-C22

ARMOR OFFICER CAREER COURSE

MOS: Prefix digit 5
added to current MOS

Length: Peacetime—36 weeks

Mobilization—None

APPROVED BY
COMMANDING GENERAL, UNITED STATES CONTINENTAL ARMY COMMAND

10 August 1961

Minor Revision—11 May 1962

This POI supersedes POI for Armor Officer Career Course, July 1961

SECTION I—PREFACE

A. Course: 17-A-C22, Armor Officer Career.

B. Purpose: To provide branch training and a working knowledge in the duties and responsibilities of Armor officers and to qualify students as nuclear weapons employment officers. MOS for which trained: Prefix digit 5 (Nuclear Weapons Employment) added to current MOS of officers who successfully complete the nuclear weapons employment phase of the course.

C. Prerequisites: Commissioned officer. Member of the active Army, whose branch is Armor. Minimum of 3 years and preferably not more than 8 years of commissioned service, (including only promotion list service for Regular Army officers). Credit for the Armor Officer Orientation Course (17-A-C20), or equivalent. Security clearance to include SECRET (final). Obligated service for active Army officers: 1 year.

	Peacetime	Mobilization
D. Length:	36 weeks	None
E. Training Locations:	US Army Armor School	None
F. Percentage of Training Requirement to be School Trained:	100%	None

G. MOS Feeder Pattern:

Prequisite MOS	MOS Trained in This Course	Feeds Following MOS
None	Prefix digit 5 added to current MOS	None

H. Ammunition Requirements: See section V.

I. Common Subjects Recapitulation: See section VI.

J. Standardization of Prefix Digit 5 Training: See section VII.

SECTION II—SUMMARY
Armor Officer Career Course
Peacetime: 36 weeks, 1,584 hours
Mobilization: None

Subject	Hours	Annex	Page
A. Academic Subjects			
1. Automotive Department	60		
Automotive Subjects	60	1	12
2. Command and Staff Department	695		
a. Tank and Mechanized Infantry Tactics	274	2A	17
b. Armored Cavalry	83	2B	27
c. Army Aviation	15	2C	30
d. Staff Subjects	74	2D	31
e. Artillery Operations	25	2E	36
f. Engineer Operations	19	2F	37
g. Amphibious Operations	20	2G	40
h. USAF Operations	5	2H	41
i. Nuclear Weapons Employment	150	2I	42
j. Nuclear Weapons Employment (Foreign Officers)	*48	2J	47
k. Examinations	20	2K	49
Night Attack (Supplemental Training)	(4)	2A	27
3. Communication Department	71		
a. Equipment and Procedure	36	3A	49
b. Tactical Communication	13	3B	53
c. Field Communication	22	3C	54
4. General Subjects Department	132		
a. Military Leadership	5	4A	56
b. Code of Conduct	1	4A	56
c. Survival, Escape, and Evasion	1	4A	57
d. Character Guidance	1	4A	57
e. Duties of the Army Advisor	1	4A	57
f. Military Justice	8	4B	57
g. Military History	17	4C	58
h. Physical Training	8	4D	58
i. Map and Airphoto Reading	23	4E	59
j. Military Writing	16	4F	60
k. Training Management	21	4G	61
l. Army Management	4	4G	61
m. Domestic Emergencies and Civil Defense	9	4H	62
n. Medical Services	8	4I	63
o. Psychological Warfare	1	4J	64
p. Civil Affairs and Counterinsurgency	6	4J	64
q. Examination and Critique	3	4K	64
Map Reading (Supplemental Training)	(8)	4E	59
5. Weapons Department	109		
a. Arms Division	20	5A	65
b. Gunnery Division	89	5B	66

*Not included in overall total.

SECTION I—PREFACE

A. Course: 17-A-C22, Armor Officer Career.

B. Purpose: To provide branch training and a working knowledge in the duties and responsibilities of Armor officers and to qualify students as nuclear weapons employment officers. MOS for which trained: Prefix digit 5 (Nuclear Weapons Employment) added to current MOS of officers who successfully complete the nuclear weapons employment phase of the course.

C. Prerequisites: Commissioned officer. Member of the active Army, whose branch is Armor. Minimum of 3 years and preferably not more than 8 years of commissioned service, (including only promotion list service for Regular Army officers). Credit for the Armor Officer Orientation Course (17-A-C20), or equivalent. Security clearance to include SECRET (final). Obligated service for active Army officers: 1 year.

	Peacetime	Mobilization
D. Length:	36 weeks	None
E. Training Locations:	US Army Armor School	None
F. Percentage of Training Requirement to be School Trained:	100%	None

G. MOS Feeder Pattern:

Prequisite MOS	MOS Trained in This Course	Feeds Following MOS
None	Prefix digit 5 added to current MOS	None

H. Ammunition Requirements: See section V.

I. Common Subjects Recapitulation: See section VI.

J. Standardization of Prefix Digit 5 Training: See section VII.

SECTION II--SUMMARY
Armor Officer Career Course
Peacetime: 36 weeks, 1,584 hours
Mobilization: None

Subject	Hours	Annex	Page
A. Academic Subjects			
1. Automotive Department	60		
Automotive Subjects	60	1	12
2. Command and Staff Department	685		
a. Tank and Mechanized Infantry Tactics	274	2A	17
b. Armored Cavalry	83	2B	27
c. Army Aviation	15	2C	30
d. Staff Subjects	74	2D	31
e. Artillery Operations	25	2E	36
f. Engineer Operations	19	2F	37
g. Amphibious Operations	20	2G	40
h. USAF Operations	5	2H	41
i. Nuclear Weapons Employment	150	2I	42
j. Nuclear Weapons Employment (Foreign Officers)	*48	2J	47
k. Examinations	20	2K	49
Night Attack (Supplemental Training)	(4)	2A	27
3. Communication Department	71		
a. Equipment and Procedure	36	3A	49
b. Tactical Communication	13	3B	53
c. Field Communication	22	3C	54
4. General Subjects Department	132		
a. Military Leadership	5	4A	56
b. Code of Conduct	1	4A	56
c. Survival, Escape, and Evasion	1	4A	57
d. Character Guidance	1	4A	57
e. Duties of the Army Advisor	1	4A	57
f. Military Justice	8	4B	57
g. Military History	17	4C	58
h. Physical Training	8	4D	58
i. Map and Airphoto Reading	23	4E	59
j. Military Writing	16	4F	60
k. Training Management	31	4G	61
l. Army Management	4	4G	61
m. Domestic Emergencies and Civil Defense	9	4H	62
n. Medical Services	8	4I	63
o. Psychological Warfare	1	4J	64
p. Civil Affairs and Counterinsurgency	5	4J	64
q. Examination and Critique	3	4K	64
Map Reading (Supplemental Training)	(8)	4E	59
5. Weapons Department	109		
a. Arms Division	20	5A	65
b. Gunnery Division	89	5B	66

*Not included in overall total.

Subject		Hours	Annex	Page
6. Senior Officer's Preventive Maintenance Department		14		
a. Command Aspects of Preventive Maintenance		7	6A	70
b. Concept of PM Indicators		7	6B	71
7. Office of Director of Instruction		103		
a. Methods of Instruction		27	7A	73
b. Educational Development		7	7B	74
c. Nonresident Instruction and Training Assistance		1	7C	75
d. Guest Speaker Program		68	Omitted	
	Subtotal	1,174		
B. Nonacademic Subjects				
1. Inprocessing		20		
2. Outprocessing		11		
3. Graduation		1		
4. Physical Conditioning		136		
5. Commandant's Time		72		
6. Open Time		170		
	Subtotal	410		
	Total	1,584		
C. Recapitulation				
1. Security classification				
SECRET		189		
CONFIDENTIAL		20		
Unclassified		1,375		
	Total	1,584		
2. Type of Instruction				
Conference (C)		398		
Demonstration (D)		71		
Practical Exercise (PE)		627		
Examination (E)		56		
Lecture (L)		22		
Nonacademic		410		
	Total	1,584		
D. Supplemental Training		(12)		
Command and Staff Department		(4)		
General Subjects Department		(8)		

APPENDIX C

ARMOR OFFICER ADVANCED COURSE PROGRAM OF INSTRUCTION

SECTION I — PREFACE

A. Course: 17-O-3 Armor Officer Advanced.

B. Purpose: To provide advanced branch training to officers so that they are thoroughly grounded in the duties and responsibilities appropriate to field grade Armor officers. MOS for which trained: Prefix digit 5 added to current MOS.

C. Prerequisites: Commissioned officer. Member of the Regular Army or a reserve component officer in an active status or on active duty whose assignment, actual or anticipated, is to Armor duties. Minimum of five years but not more than twelve years of commissioned service (including only promotion list service for Regular Army officers). Credit for an Armor company grade officer regular or associate course. Security clearance to include SECRET.

	Peacetime	Mobilization
D. Length:	36 weeks--1584 hours	None
E. Training Location:	The Armor School	None
F. Percentage of Training Requirement to be School Trained:	100%	None

G. MOS Feeder Patterns: None.

H. Ammunition Requirements: See section V.

I. Common Subjects Recapitulation: See section VI.

NOTE: Program of Instruction approved by 1st Ind ATERM 352.11 (27 July 56) Headquarters, Continental Army Command, 20 Sep 56 To Letter AICBB-A 352.11, Headquarters The Armor School, 27 July 1956, Subject, "Program of Instruction For Armor Officer Advanced Course, 17-O-3."

SECTION II--SUMMARY

ARMOR OFFICER ADVANCED COURSE

Length: Peace; 36 weeks--1584 hours

Mobilization*: None

Subject	Hours*	Annex Nr	Page Nr
A. ACADEMIC SUBJECTS			
1. Automotive Department	75		21
Automotive General	(27)	1A	21
Maintenance Administration and Inspections	(15)	1B	22
Driving and Driving Principles	(12)	1C	24
Preventive-Maintenance Services	(19)	1D	25
Examination and Critique	(2)	1E	27
2. Command and Staff Department	~~786~~ 715		28
Introduction	(1)	2A	28
Armor Employment	(235)	2B	28
(1) Team and Task Force; Combat Command and Division	~~178~~ 173		28
(2) Reconnaissance Operations	50		38
(3) Army Aviation	~~71~~		41
Air Operations	(19)	2C	42
Amphibious Operations	(18)	2D	45
Special Weapons	(82)	2E	47
Field Exercises	(112)	2F	56

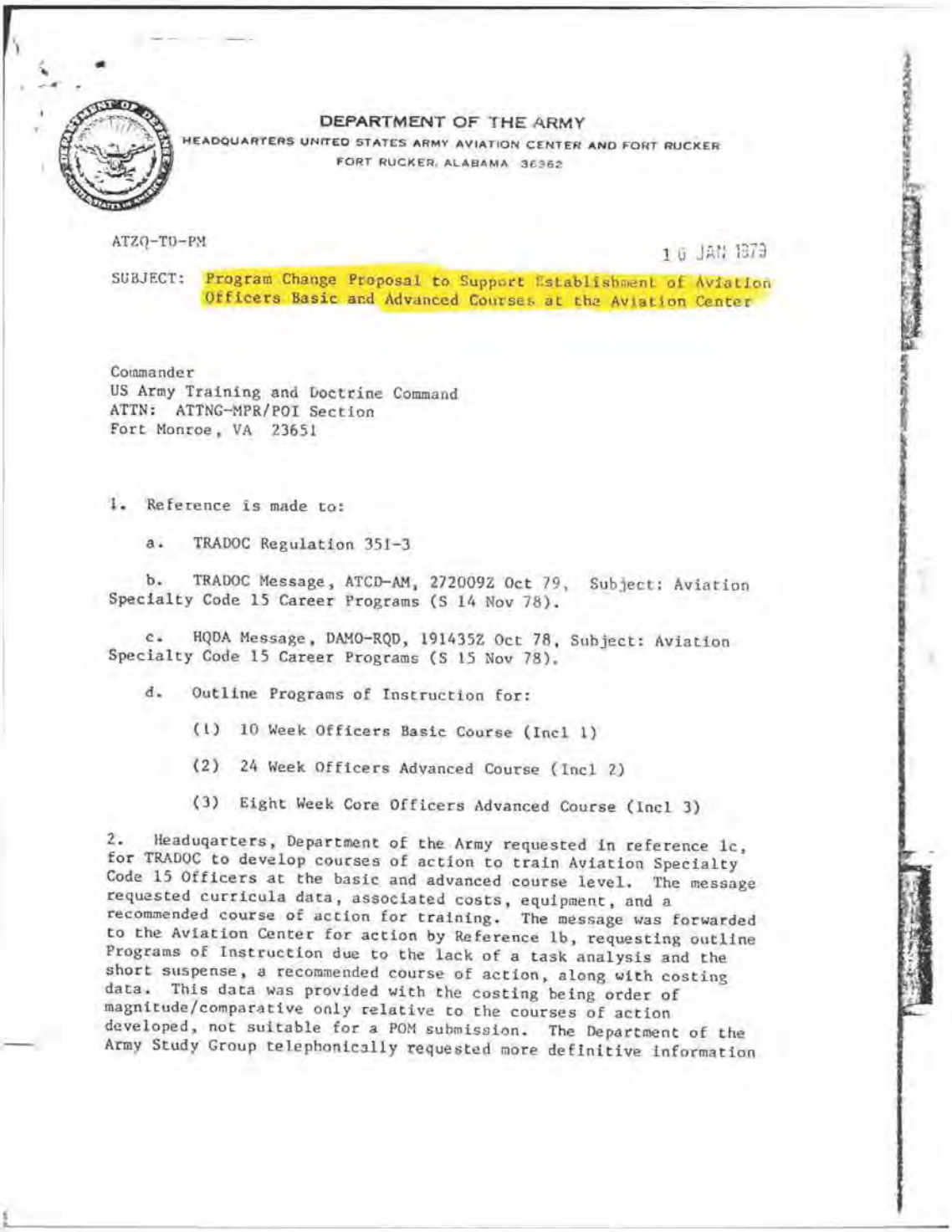
*No Mobilization Requirements in this Program of Instruction.

Subject	Hours	Annex Nr	Page Nr
Military Leadership	(7)	4E	100
Medical Training and Support	(7)	4F	101
Training Management	(20)	4G	102
Civil Emergencies	(17)	4H	103
Military Writing	(59) 58	4I	107
Readings in Military History	(18)	4J	109
Common Subjects	(6) 7	4K	110
Miscellaneous Subjects	(4)	4L	111
Department Director's Orientation	(1)	4M	112
Examination and Critique	(9)	4N	113
Guest Speaker	(14)	Omitted	
5. Weapons Department	125		114
Small Arms	(20)	5A	114
Materiel	(28)	5B	115
Tank Gunnery	(77)	5C	117
Sub-Total	1320		
B. NONACADEMIC SUBJECTS			
Physical Conditioning	(72)		
Commandant's Time	(92) 93		
Open Time	(80)		
In-Processing	(12)		
Out-Processing	(8)		
Sub-Total	264		
Total	1584		

Subject	Hours	Annex Nr	Page Nr
C. RECAPITULATION			
1. Security Classification			
SECRET	111		
CONFIDENTIAL	17		
UNCLASSIFIED	1456		
Total	1584		
2. Type of Instruction			
Conference	406		
Demonstration	99		
Practical Exercise	752		
Examinations	63		
Nonacademic Subjects	264		
Total	1584		

APPENDIX D

AVIATION PROGRAM OF INSTRUCTION MEMORANDUM



DEPARTMENT OF THE ARMY
HEADQUARTERS UNITED STATES ARMY AVIATION CENTER AND FORT RUCKER
FORT RUCKER, ALABAMA 36362

ATZQ-TD-PM

16 JAN 1979

SUBJECT: Program Change Proposal to Support Establishment of Aviation Officers Basic and Advanced Courses at the Aviation Center

Commander
US Army Training and Doctrine Command
ATTN: ATTNG-MPR/POI Section
Fort Monroe, VA 23651

1. Reference is made to:

a. TRADOC Regulation 351-3

b. TRADOC Message, ATCD-AM, 272009Z Oct 79, Subject: Aviation Specialty Code 15 Career Programs (S 14 Nov 78).

c. HQDA Message, DAMO-RQD, 191435Z Oct 78, Subject: Aviation Specialty Code 15 Career Programs (S 15 Nov 78).

d. Outline Programs of Instruction for:

(1) 10 Week Officers Basic Course (Incl 1)

(2) 24 Week Officers Advanced Course (Incl 2)

(3) Eight Week Core Officers Advanced Course (Incl 3)

2. Headuqarters, Department of the Army requested in reference 1c, for TRADOC to develop courses of action to train Aviation Specialty Code 15 Officers at the basic and advanced course level. The message requested curricula data, associated costs, equipment, and a recommended course of action for training. The message was forwarded to the Aviation Center for action by Reference 1b, requesting outline Programs of Instruction due to the lack of a task analysis and the short suspense, a recommended course of action, along with costing data. This data was provided with the costing being order of magnitude/comparative only relative to the courses of action developed, not suitable for a POM submission. The Department of the Army Study Group telephonically requested more definitive information

ATZQ-TD-PM

SUBJECT: Program Change Proposal to Support Establishment of Aviation Officers Basic and Advanced Courses at the Aviation Center

to include data for possible POM submissions as part of a Decision Briefing for the Chief of Staff, Army, scheduled for 23 January 1979. The Study Group requested data on only three courses of action. These three courses are: an Officers Basic Course taught in conjunction with the Initial Entry Rotary Wing Flight Training Course with the course length to be less than one year; An Officers Advanced Course of approximately six months duration similar to other Officers' Advanced Courses; and a "Core" Advanced Course which could be presented in conjunction with other alternate specialty training courses prior to an alternate specialty assignment.

3. Assumptions were required to develop these courses. The listing of the assumptions is at Inclosure 4.

4. Aviation Officers Basic Course:

a. Course: Aviation Officers Basic Course.

b. Location: United States Army Aviation Center, Fort Rucker, Alabama 36362.

c. Purpose: To provide newly accessed Commissioned Officers with the information, tactics, mission requirements, mission planning, Army organizations, tactics and employment; Aviation Units organization, missions, tactics, capabilities, doctrine and employment; Aviation unit staff functions, maintenance, supply and administration, safety, maintenance procedures and practices, to prepare to lead and employ Army Aviation in support of the Army in the field.

d. Length of Course.

(1)	Weeks	10
(2)	Hours	408
(3)	Academic	347
(4)	Non-Academic	61

e. Scope of Instruction: Academic instruction to include training and information in the following subjects: Common military tasks, military organization and leadership; command and staff procedures; maintenance and supply management; combined arms operations, general aviation subjects, application of planning of

aviation section/platoon operations, total inprocessing as a new Officer, and physical conditioning.

f. Prerequisites: Active Army and Reserve Components, qualified and selected for accession into the Aviation Specialty either upon entry upon active duty or from the field. Obligation of four years is assumed upon completion of the course. Security clearance- Secret. MOS awarded upon completion of this course and flight training, Aviation Specialty 15.

g. Proposed Class Capacity and Frequency: Class size not to exceed 30 students per class. Class frequency to be every ten training days taught to flow, after the first four weeks of the basic course, into the Initial Entry Rotary Wing Flight Training course with the remaining six weeks of the basic course being completed after completion of the flight training portion.

h. Justification for the Course: Directed to develop proposed Program of Instruction and costing data along with resources/supplies for the course as part of a Department of the Army Study effort on Aviation Specialty Code 15 Career Development.

i. Resource Requirements:

(1) Estimated fund requirements: See Incl 5.

(2) Equipment requirements: See Incl 6.

(3) Manpower requirements are: FY 80, 30; FY 81, 47; FY 82, 47. See Incl 7.

(4) Facilities Requirements: Minor Engineer work only is initially required to refurbish World War II temporary buildings as classrooms. The establishment of a Basic Course does place a long term MCA requirement for construction of a class room building. The cost of a five class room, 50 seats per class room, air-conditioned building has been estimated to cost $ 918,000.

(5) Ammunition requirements: Small arms for weapons qualifications and smoke grenades only, totals $13,300 per year.

(6) Flying time required in course: Flight hours are programmed into the course to allow application of basic course training to practical field training. This is for 8 flight hours per

student and requires five UH-1 Helicopters.

5. Aviation Officers 24 week Advanced Course.

a. Course: Aviation Officers Advanced Course (24 Week).

b. Location: United States Army Aviation Center, Fort Rucker, Alabama 36362.

c. Purpose: To provide the advanced course level training in aviation systems, employment, doctrine, the combined arms team, integration of aviation into offensive and defensive operations of the Mechanized, Armor, Air-Mobile, Infantry, and Armor Operations. Aviation Staff planning, staff operations and procedures; maintenance management and supply operations, leadership and command functions at the advanced course level in preparation for positions of higher responsibility.

d. Length of course:

(1)	Weeks	24
(2)	Hours	1000
(3)	Academic	888
(4)	Non-Academic	112

e. Scope of Instruction: Academic instruction to include training/information and practical exercises in Army aviation employment, management and leadership, training programs development, staff functions and responsibilities; the combined arms team on the modern battlefield, simulation field training exercises and staff planning through the use of the "Battle" war game simulation; threat and counter threat, aircraft survivability equipment, flight and ground safety, mission support requirements, nuclear movements, and an aviation review and update.

f. Prerequisites: Commissioned Officer from the Active or Reserve Components, Aviation Specialty Code 15 primary or alternate specialty, with a minimum of three years aviation service, rated as an Army aviator. Service Obligation: two years. Security clearance: Secret. Specialty Code for which trained: N/A.

ATZQ-TD-PM 10 JAN 1979

SUBJECT: Program Change Proposal to Support Establishment of Aviation Officers Basic and Advanced Courses at the Aviation Center

g. Proposed Class Capacity and Frequency: Class size of 130 students with two classes per year. TRADOC Form 951R, N/A.

h. Justification for Course: Outline Program of Instruction and associated costs directed to be developed by Department of the Army Study Group.

i. Resource Requirements with establishment of an Officer's Basic Course at the Aviation Center.

(1) Estimated Fund requirements: See Incl 8.

(2) Summary of Manpower: Instructor Contact Hours not presented. Summary at Incl 9.

(3) Equipment Requirements. If the Officers Basic Course is estabished, the equipment listed for that course will be utilized with this course. If the Officers' Basic course is not established, the same equipment will be required to support this course. Incl 10.

(4) Facilities Requirements: Minor Engineer effort will be required to refurbish existing World War II buildings for class rooms pending MCA construction of an appropriate permanent class room facility.

(5) Ammunition Requirements: N/A

(6) Flying time required in course: There are 24 flight hours per student programmed into the course to allow for the application of staffing planning and field training in aviation employment, tactics, techniques, and to exercise student develop plans for feasibility in execution.

j. Resource Requirements if an Officers Basic Course is not also established at the Aviation Center.

(1) Estimated fund requirements: See Incl 11.

(2) Summary of Manpower requirements: See Incl 12.

(3) Equipment Requirements: See Incl 13.

(4) Facilities Requirements: No Change from Advanced Course with Basic Course at the Aviation Center.

(5) Ammunition requirements: N/A

(6) Flying time required in course: 24 flight hours are programmed into the Aviation Officers Advanced Course for field exercises, employment in aviation tactics and tactical planning.

6. Aviation Officer Eight Week Core Advanced Courses.

a. Course: Aviation Officers Core Advanced Course.

b. Location: United States Army Aviation Center, Fort Rucker, Alabama 36362.

c. Purpose: To provide to Aviation Commissioned Officers the advanced staff planning, leadership, management, and employment doctrine, tactics, threat and counter-threat information and intensive training in the combined arms field operations and aviation support to those operations. This course would be taught in conjunction with some other training program which would provide training in a selected alternate specialty.

d. Length of course:

(1)	Weeks	8
(2)	Hours	328
(3)	Academic	288
(4)	Non-Academic	40

e. Scope of Instruction: Academic instruction to include training and field exercises will be taught in the following subjects: Detailed knowledge and employment of aviation organizations in support of Mechanized, Armor, Infantry, Air Mobile and Air-Borne operations in offensive and defensive operations as members of the combined arms team, detailed mission requirements for Attack, Utility, Cargo and Scout/Observation Helicopter missions, aerial surveillance and target acquisition missions, ASA and other support missions. A computer driven field training exercise utilizing the "Battle" simulation war game through computer terminal, Aviation Staff and command requirements for the advanced course level.

f. Prerequisites: Commissioned Officer of the Active or

Reserve Components, Aviation Specialty Code 15 primary or alternate specialty, with a minimum of three years of aviation experience, rated as an Army Aviator. Service Obligation two years. Security Clearance- Secret. Specialty Code for which trained- N/A.

g. Proposed class size: 44 students per class, a class starts every eight weeks- six per year.

h. Justification for Course: Outlined program of instruction along with associated costs directed to be developed by Department of the Army Study Group.

i. Resource Requirements if an Aviation Officer Basic Course is established at the Aviation Center.

(1) Estimated fund requirement: See Incl 14.

(2) Summary of Manpower: See Incl 15.

(3) Equipment Requirements: See Incl 16.

(4) Facilities Requirements: Minor engineering effort required to refurbish existing World War II buildings for class rooms pending MCA construction of a permanent class room building.

(5) Ammunition Requirements: N/A.

(6) Flying time required in course: Eight hours per student is programmed into the course to allow for training in new developments, tactics and techniques and to field verify staff planning of aviation employment.

j. Aviation Officers Advanced Core Course if the Basic Officers Course is not also established at the Aviation Center.

(1) Estimated fund requirement: See Incl 17.

(2) Summary of Manpower: See Incl 18.

(3) Equipment Requirements: See Incl 19.

(4) Facilities requirements: Minor Engineer effort to refurbish World War II Buildings into class rooms until construction of permanent facilities under MCA appropriations.

ATZQ-TD-PM 10 JAN 1979
SUBJECT: Program Change Proposal to Support Establishment of Aviation Officers Basic and Advanced Courses at the Aviation Center

(5) Ammunition Requirements- N/A

(6) Flying time required in course: Same as with basic course established at the Aviation Center.

7. The task analysis to support Aviation Specialty Code 15 is programmed for FY 79. As this task analysis is being developed, there will be changes in the task list. These changes in the tasks required to be taught in the courses would require changes in the curricula for the above courses. These changes would also impact on resources. If it is the decision to utilize any of these courses, a further refinement of the Programs of Instruction and additional Program Change Proposals would be required prior to final implementation of the courses.

8. The start date for training for a Basic Course should not be planned prior to FY 1981. This gives time for the completion of the task analysis, and with utilization of existing course materials modified for use at the Aviation Center, development of all course materials. If a full Instructional Systems Development application is utilized for the Specialty Code 15, the TRADOC developed model of 30 months should be utilized to establish the start dates.

9. A prior request has been submitted for an Attack Helicopter Company, an Air Traffic Control Company and a Field Artillery Battery to be assigned to the Aviation Center for school support. The requirement for these units is reinforced if either the basic or advance courses were established.

FOR THE COMMANDER:

Lyle E. Tuttle CPT AGC
[illegible] DAC
Assistant Adjutant General

19 Incl
as

Section 2: Summary

AVIATION OFFICER BASIC COURSE

Phase: 408

SUBJECT		HOURS	ANNEX
A. Academic Subjects			
Common Military Tasks	Annex Total	91	A
Organization and Leadership	Annex Total	21	B
Command and Staff	Annex Total	28	C
Maintenance and Supply Management	Annex Total	56	D
Combined Arms Operations	Annex Total	84	E
General Aviation Subjects	Annex Total	35	F
Flight Training	Annex Total	24	G
*Simulated Flight Training	Annex Total	8	H
	Total	347	
B. Non Academic Subjects			
In Processing		16	
Out Processing		4	
Physical Conditioning		25	
Open Time		16	
	Total	61	
C. Recapitulation			
1. Security Classification			
Secret		2	
Confidential		2	
Unclassified		404	
	Total	408	
2. Type of Instruction			
Case study		30.0	
Conference		111.0	
Demonstration		10.0	
Examination 1		10.0	
Examination 2		15.0	
Self Pace		14.0	
Examination 3		15.0	
Film/TV		1.0	

NOTE: Training to be scheduled after normal duty hours.

Practical exercise 1		42.0
Practical exercise 2		42.0
Practical exercise 3		44.0
Programmed Instruction		1.0
Seminar		4.0
Exam Analysis		61.0
	Total	405.0

SSGT104 3. Daly

ANNEX A Common Military Task

Purpose: To provide the student with a general knowledge of tasks which are common to military units, including military life, map reading, military law, NBC, SAFE, Ground Tactical Communications, and Weapons Qualification.

		Class	Type of Instruction			
Hours:	91	U	46	46S	21C	1r 40
			1P1	14SP	5PE1	10P32
			8W3	8C1	7H2	4H5

ANNEX B Organization and Leadership

Purpose: To provide the student with a general knowledge of Military Organization, Organizational Effectiveness, and Military Leadership.

		Class	Type of Instruction		
Hours:	21	U	12C5	7P62	2H3

ANNEX C Command and Staff

Purpose: To provide the student with a general knowledge of the role of the commander and the functions of staff and staffing procedures.

		Class	Type of Instruction			
Hours:	28	U	13C	3C5	7PE3	5H3

ANNEX D Maintenance and Supply Management

Purpose: To provide the student with the general outline of Army Maintenance Management and Logistics structure and to provide specific instruction in the application of Maintenance and Supply procedures.

		Class	Type of Instruction			
Hours:	56	U	8C	11C5	7P	13P61
			14P63	2H1	4H2	2H3

ANNEX E Combined Arms Operations

Purpose: To provide the student with a background in [illegible] Forces, operations and capabilities, and acquaint the student with allied, joint, and Combined Arms Operations and Procedures.

		Class	Type of Instruction
Hours:	85	2S, 32U	3[illegible] 2[illegible] [illegible] 4[illegible] 3[illegible] -

ANNEX F General Aviation Subjects

Purpose: To provide the student with a basic knowledge of Air Cavalry, Attack, Air Assault, and Assault Support Operations to include an introduction to Offensive and Defensive Operations and the High Threat environment.

		Class	Type of Instruction
Hours:	35	2S, 33U	31C 4[illegible]

ANNEX G Flight Training

Purpose: To maintain individual proficiency and currency of aviation skills taught in O[illegible].

		Class	Type of Instruction
Hours:	24	U	24[illegible] (19[illegible], 5[illegible])

ANNEX H Simulated Flight Training

Purpose: To provide minimum simulated flight training requirements.

		Class	Type of Instruction
Hours:	8*	U	S[illegible] (3.0S:[illegible]S)

*NOTE: Training to be scheduled after normal duty hours.

SECTION 2 SUMMARY

AVIATION OFFICER ADVANCED COURSE

Hour A 1000

Subject			Hours	Annex
A.	Academic Subjects:			
	Profession of Arms	Annex Total	252	A
	Military Arts	Annex Total	203	B
	Aviation Review	Annex Total	175	C
	Army Aviation Employment	Annex Total	87	D
	Simulated Aviation FTX	Annex Total	35	E
	Flight Training	Annex Total	95	F
	*Simulated Flight Training	Annex Total	40	G
		Total	888	
B.	Non Academic Subjects			
	In Processing		16	
	Out Processing		8	
	DA Personnel Management Briefing		8	
	Physical Conditioning		40	
	Commandant's Time		24	
	Open Time		16	
		Total	112	
C.	Recapitulation			
	1. Security Classification			
	Secret		50	
	Confidential		20	
	Unclassified		930	
		Total	1000	
	2. Type of Instruction			
	Case Study		24.0	
	Conference		351.0	
	Demonstration		2.0	
	Examination 1		4.0	
	Examination 3		24.0	

Sect 2

Film/TV	23.0
Practice Exercise 1	36.0
Practice Exercise 2	155.0
Practice Exercise 3	102.6
Programmed Instruction	4.0
Seminar	97.6
Computer Assisted Instruction	35.0
Not Available	112.0
Total	1059.0

*NOTE: Training to be scheduled after normal duty hours.

SECTION 3 SUBJ

AVIATION OFFICER ADVANCED COURSE

ANNEX A THE PROFESSION OF ARMS

PURPOSE: To provide the student with a basic knowledge in the areas of Management/Leadership, Financial Management, Personnel Management, Logistics Management, Maintenance Management, Contemporary Subjects, Communicative Arts, and General Subjects.

		Class	Type of Instruction					
HOURS:	252	U	100.0	C	33.0	S		
			8.0	CS	10.0	TV/F		
			16.0	PE1	56.0	PE2		
			42.0	PE3	13.0	E3		

ANNEX B MILITARY ARTS

PURPOSE: To provide the student with a basic working knowledge of Strategy, Intelligence, Operations, Combined Arms, and Special Subjects.

		Class	Type of Instruction					
HOURS:	203	178U, 25S	105.0	C	25.0	S		
			10.0	TV/F	32.0	PE3		
			3.0	PE2	4.0	PI	2.0	D
			4.0	E1	12.0	CS	5.0	E3

ANNEX C AVIATION REVIEW

PURPOSE: To provide the student with a basic knowledge of Structure, Present Role and Developments. Also provide a general knowledge of Aviation related subjects which include Communications, Aviation Medicine, Roles of Allied Services, Command and Control, and Aviation Safety/Accident Investigation.

		Class	Type of Instruction					
HOURS:	175	170U, 5S	113.0	C	18.0	PE3		
			8.0	PE1	4.0	CS	8.0	S
			17.0	PE2	3.0	TV/F		
			4.0	E3				

ANNEX D ARMY AVIATION EMPLOYMENT

PURPOSE: To provide student with specific knowledge to enable him to employ the various types of aviation assets and units. Aviators will be trained in their track of either Cargo Helicopter Operations, Utility Helicopter Operations, Observation Helicopter Operations or Attack Helicopter Operations.

		Class	Type of Instruction			
HOURS:	87	670, 155, 50	32.0	C	10.0	PE3
			31.0	S	2.0	E3
			12.0	PE1		

ANNEX E SIMULATED AVIATION FIX

PURPOSE: To provide the student with the concepts of employing Aviation assets in support of the ground elements of the combined arms on the modern battle field using simulated gaming devices.

		Class	Type of Instruction	
HOURS:	35	150, 105, 100	35.0	CAI

ANNEX F FLIGHT TRAINING

PURPOSE: To allow the student to maintain proficiency and be trained in new developments in the employment of aviation assets.

		Class	Type of Instruction
HOURS:	96	U	96 PE2 (8.0 DF 16.0 SF)

ANNEX G SIMULATED FLIGHT TRAINING

PURPOSE: To provide minimum simulated flight training requirements.

		Class	Type of Instruction
HOURS:	40	U	40 PE2 (10 STS)

SECTION 2: SUMMARY

AVIATION OFFICER ADVANCED COURSE
(Aviation Core Alternative)

Hours 328

Subject		Hours	Annex
A. Academic Subjects			
Aviation Review	Annex Total	123	A
Army Aviation Employment	Annex Total	90	B
Simulated Aviation FTX	Annex Total	35	C
Flight Training	Annex Total	32	D
*Simulated Flight Training	Annex Total	8	E
	Total	288	
B. Non Academic Subjects			
In Processing		8	
Out Processing		8	
DA Personnel Management Briefing		8	
Physical Conditioning		8	
Commandant's Time		8	
	Total	40	
C. Recapitulation			
1. Security Classification			
Secret		20	
Confidential		19	
Unclassified		289	
	Total	328	
2. Type of Instruction			
Case Study		4	
Conference		96	
Examination 3		6	

*NOTE: Training will be scheduled after normal duty hours.

Film/TV	3
Practice Exercise 1	20
Practice Exercise 2	57
Practice Exercise 3	28
Seminar	39
Computer Assisted Instruction	35
Non Academic	40
Total	328

*NOTE: Training will be scheduled after normal duty hours.

SECTION 3 -- BODY

AVIATION OFFICER ADVANCED COURSE
(Aviation Core Alternative)

ANNEX A AVIATION REVIEW

PURPOSE: To provide the student with a basic knowledge of Aviation Structure, Present Role and Developments. Also provide a general knowledge of Aviation related subjects which include Communications, Aviation Medicine, Roles of Allied Services, Command and Control, and Aviation Safety/Accident Investigation.

		Class	Type of Instruction				
HOURS:	123	4C, 119U	61.0	C	18.0	PE3	
			8.0	PE1	4.0	CS	8.0 S
			17.0	PE2	3.0	TV/F	
			4.0	E3			

ANNEX B ARMY AVIATION EMPLOYMENT

PURPOSE: To provide student with specific knowledge to enable him to employ the various types of aviation assets and units. Aviators will be trained in their track of either Cargo Helicopter Operations, Utility Helicopter Operations, Observation Helicopter Operations or Attack Helicopter Operations.

		Class	Type of Instruction			
HOURS:	90	75U, 10S, 5C	35.0	C	10.0	PE3
			31.0	S	2.0	E3
			12.0	PE1		

ANNEX C SIMULATED AVIATION FOX

PURPOSE: To provide the student with the concepts of employing Aviation assets in support of the ground elements of the combined arms team on the modern battle field using simulated gaming devices.

		Class	Type of Instruction	
HOURS:	35	15U, 10S, 10C	35.0	CAI

ANNEX D FLYING

PURPOSE: To allow the student to maintain proficiency and be trained in new developments in the employment of aviation assets.

	Class	Type of Instruction
HOURS:	32	U 32P E2 (2.0 DF, 6.0SF)

ANNEX E SIMULATED FLIGHT TRAINING

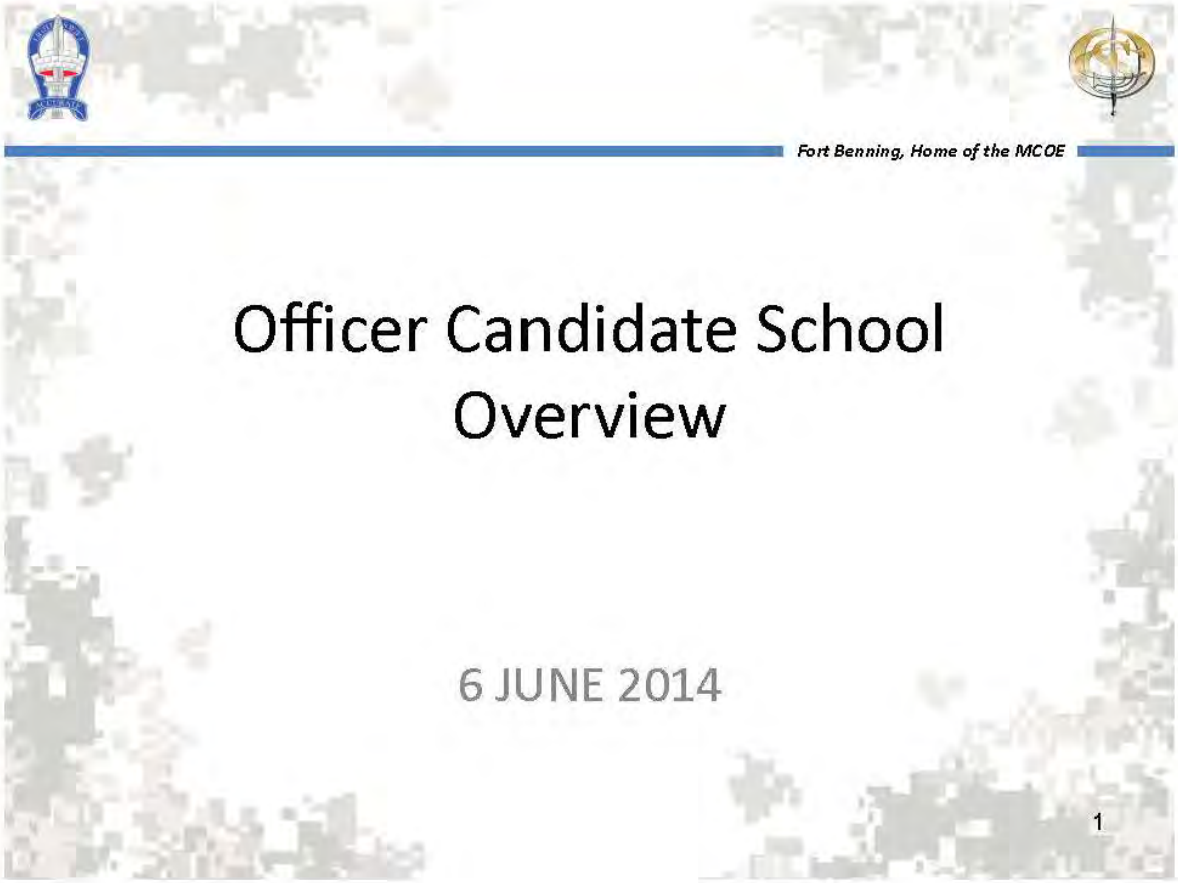
PURPOSE: To provide the trainee simulated flight training requirements.

	Class	Type of Instruction
HOURS:	8*	U 8 PE2 (3.5 SFTS)

*NOTE: Training to be scheduled after normal duty hours.

APPENDIX E

TWELVE-WEEK TRANING PLAN OFFICER CANDIDATE SCHOOL



TYPICAL DAY

Fort Benning, Home of the MCOE

- 0545 First formation
- 0600-0700 Physical training
- 0700-0715 Personal hygiene
- 0730-0800 Breakfast
- 0800-1115 Training/Classes
- 1130-1200 Lunch
- 1200-1645 Training/Classes
- 1700-1730 Dinner
- 1730-2100 Study barracks
- 2100-2200 Personal time
- 2200 Lights out

-SUNDAY Religious Services – Student must fill out a trip ticket by Thursday of that week

2

WEEK 1-3 OVERVIEW

Fort Benning, Home of the MCOE

- Initial APFT
- Individual Skills
- Bolton Obstacle/Confidence Course
- Combat Water Survival Test (CWST)
- Leadership and Ethics
- 6 mile foot march, 3 mile release run
- Leader's Reaction Course
- Map Reading and Land Navigation

3

WEEK 4-6 OVERVIEW

Fort Benning, Home of the MCOE

- 8 and 10 mile Foot Marches, 3 mile release run, Combatives
- WTBDs & CFF
- Military intelligence
- Tactics and operations
- Terrain Walk
- Squad FLX

WEEK 7-9 OVERVIEW

Fort Benning, Home of the MCOE

- 12 Mile Foot March / Crucible
- FLX
- Recovery operations
- Branch selection
- Military History
- Training management and CSDP
- Leadership

WEEK 10-12 OVERVIEW

Fort Benning, Home of the MCOE

- ❖ Branch mentorship
- ❖ Andersonville Staff Ride
- ❖ Final APFT
- ❖ Maneuver/ Mentorship/ Graduation Runs
- ❖ Senior Leader Seminars
- ❖ Transitioning to becoming Commissioned Officers…Graduation Social, Graduation Formal, Graduation

6

OCS GRADUATION REQUIREMENTS

Fort Benning, Home of the MCOE

- ❑ Meet Army height & weight standards
- ❑ Pass three APFTs – initial, mid-cycle, & final
- ❑ Obstacle Confidence Course
- ❑ Combat Water Survival Test (CWST)
- ❑ Achieve above 80% on 9 academic tests
- ❑ Pass day/night land navigation test
- ❑ Complete two 3-mile release runs (timed events)
- ❑ Complete one 6-mile, one 8-mile, one 10-mile and one 12-mile foot march
- ❑ Pass 70% of evaluated leadership positions (Garrison & Field)

7

APPENDIX F

CYBER ADVANCE SHEET

US ARMY COMMAND AND GENERAL STAFF COLLEGE
US Army Command and General Staff School
Command and General Staff Officers Course (CGSOC) Common Core
C300: Unified Action within Operational Art

Advance Sheet for Lesson C310
Cyberspace Operations

1. SCOPE

The objective of this 2-hour lesson is to help you understand the fundamentals of cyberspace operations through preparatory readings followed by classroom discussion and in-class exercises. This lesson will allow you to comprehend and use the fundamentals of cyberspace operations related to unified action, joint force organizations, joint command authorities; and the relations between the Combatant Commands (CCMDs), Strategic Command (STRATCOM) and its sub-unified command Cyber Command (CYBERCOM). Upon completion of this lesson, you will comprehend cyber functions, capabilities and limitations; and how cyber operations are integrated in joint planning for unified action.

2. LEARNING OBJECTIVES

This lesson supports TLO-CC-5. Explain joint operations fundamentals, capabilities, limitations, and considerations of joint forces, and interorganizational and multinational partners for joint and multinational operations.

ELO-CC-5.11
Action: Explain U.S. Cyber functions, capabilities, limitations and considerations relevant to planning and conducting military operations.
Conditions: Using joint doctrinal and other readings, references, research, class discussion, personal experience, and practical exercise materials for joint and multinational operations planning and execution at the strategic and operational levels.
Standards: Explanation includes–
1. Cyber functions, capabilities and limitations; and,
2. Cyber command and control considerations in support of the Joint Force Commander.

Learning Domain: Cognitive **Level of Learning**: Comprehension

JPME I Learning Areas Supported:

1b. Comprehend the framework within which joint forces are created, employed, and sustained in support of JFCs and their component commanders.
1c. Comprehend the purpose, roles, functions and relationships of the President and the SecDef, National Security Council (NSC), Homeland Security Council, CJCS, JCS, combatant commanders, joint force commanders (JFCs), Service component commanders and combat support organizations or agencies.
1d. Comprehend joint force command relationships.
1e. Comprehend how the US military is organized to plan, execute, sustain and train for joint, interagency, intergovernmental, and multinational operations.
2a. Comprehend current joint doctrine.
2b. Comprehend the factors and emerging concepts influencing joint doctrine.
2c. Apply solutions to operational problems using current joint doctrine.
2d. Comprehend the interrelationship between Service doctrine and joint doctrine.

3a. Comprehend the considerations for employing joint and multinational forces at the operational level of war.
3b. Comprehend the interrelationships among the strategic, operational and tactical levels of war.
4a. Comprehend the relationship among national objectives and means available through the framework provided by national level systems.
4b. Comprehend the fundamentals of joint operation planning.
4c. Comprehend the effect of time, coordination, policy changes and political development on the planning process.

3. ASSIGNED STUDENT READINGS: You will find these readings on Blackboard C310 lesson material.

First Requirement:

Read:
C310RA. "Joint Information White Paper" signed by General Martin Dempsey, 22 January 2013(6 pages). Read to understand the context for cyber operations in the joint information environment.

C310RB. FM 3-38 extract. (~10 pages) **(NOTE:** Read highlighted text in the extract, primarily to understand joint doctrinal aspects of cyber operations.

C310RC. Brett, Williams T. (MG), "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly*, Issue 73, 2nd QTR 2014 12-19. (~8 pages) Read to understand cyberspace operations and contribute during discussion and in-class exercises.

Second Requirement: Come to class prepared to discuss the following topics:

- What are Cyber, Cyber Operations and Cyberspace?
- What is the importance of the Joint Information Environment (JIE)?
- What is the Cyberspace Domain, its characteristics and relationship amongst other domains?
- What the functions of Cyberspace Operations? How are they interdependent, vulnerable and what are their shortfalls?
- What are cyber joint operations considerations?
- How is Cyberspace operations related to mission command?
- What is the cloud and how will it enable cyber activities?
- What are the theories/implications of MG Brett T. William's article on cyberspace operations?

5. ASSESSMENT PLAN

Contribution to Learning and C300 Theme Exam.

APPENDIX G

KANSAS STATE UNIVERSITY OUTREACH TO DEPARTMENT OF DEFENSE

Kansas State University

DoD Information Assurance Scholarship Program
Annex II - Capacity Building
Technical Proposal

B. Project Name: Outreach to Department of Defense

1. Project Description:

Our society has become increasingly reliant on digital devices and computer network infrastructures for day-to-day decision-making. With escalating threats coming from the cyberspace,[2,3,4] it has become imperative for *everyone* to obtain necessary education and training in information assurance and cybersecurity. There is an increasing demand from both the civilian and military sectors to provide cyber-security education and hands-on training to students from all backgrounds, not limited to those in science and engineering alone. Such educational efforts are essential in effectively leveraging information technology to enhance our national work force and the nation's military capability in modern warfare. The Center for Information and Systems Assurance (CISA) at Kansas State University was recently designated as a Center of Academic Excellence of Information Assurance Research (CAE-R) by the NSA and DHS. Through our interactions with the U.S. Army Command and General Staff College (CGSC) we have identified the need for a comprehensive cybersecurity curriculum that balances foundational and practical knowledge, but neither of the two institutions currently possesses detailed curricula to accomplish this. The proposed project will leverage K-State faculty's expertise in the area of cybersecurity to develop a curriculum that fits the needs of the students at both K-State and CGSC.

While most computer science departments offer computer security courses, their content and pace is often not suitable for students outside computer science. Although these students do not have or need in-depth understanding of computing systems, their daily work/studies-related activities may be tightly integrated with, and dependent on cyber-infrastructure, e.g. creating and maintaining data collections and managing information flow within their organizations. Cybersecurity education is therefore crucial, but we must take into account students' different levels of expertise and understanding of the cyber-infrastructure. The contributions of the proposed activity are two-fold: (a) **to develop a comprehensive cybersecurity curriculum which addresses the challenge of educating and providing hands-on training to students of broad academic backgrounds**, and (b) **to design courses with innovative modules and lesson plans based on lab exercises, warfare and cyber-threat scenarios which can seamlessly integrate security education throughout different parts of students' existing information technology curriculum**.

---

[2] Devlin Barrett. Hackers Penetrate Nasdaq Computers. Wall Street Journal, February 5, 2011. http://online.wsj.com/article/SB10001424052748704709304576124502351634690.html

[3] CBS Interactive Staff. DoD Gates: We're always under cyberattack. ZDNet, April 22, 2009. http://www.zdnet.com/news/dod-gates-were-always-under-cyberattack/290770

[4] Siobhan Gorman, August Cole, and Yochi Dreazen. Computer Spies Breach Fighter-Jet Project. Wall Street Journal, April 21, 2009. http://online.wsj.com/article/SB124027491029837401.html

Our collaboration with CGSC provides an excellent opportunity to educate students who, while having diverse backgrounds, are in clear need of cybersecurity knowledge in their career. The differences in missions and curriculum structures between K-State and CGSC in terms of course duration, contents, and outcomes will allow implementation and evaluation of our innovative course modules. In addition to increasing the number of cybersecurity-savvy students, this project will enhance partnering institutions' faculty expertise in cybersecurity. Furthermore, CISA members have been engaged extensively in K-12 education with NSF, and K-State has funded programs such as RET, GK-12 STEM Fellows, REU, and Girls Researching Our World. The curriculum material developed under this project will be integrated and disseminated via these activities.

Another outcome of our discussions was identification of methodologies to deliver curriculum content. While the standard lecture and lab exercise format may be suitable for certain courses, others may require a more hands-on, scenario-driven approach. For instance, many organizational and information technology principles are taught at CGSC using warfare scenarios. These scenarios, already integrated into the CGSC curriculum, will allow us to integrate student exposure to cybersecurity threats at various points during their training, and teach avoidance and defense techniques. Thus, given the differences in learning techniques and in the duration/contents of existing courses at CGSC and K-State, it is imperative that our proposed curriculum contain modular lesson plans based hands-on exercises and threat scenarios, and innovative delivery techniques so that different modules can be selected and easily integrated with existing course contents at each institution.

2. Expected Objectives:

a. Short-Term Outcomes

Our strategy is to develop the curriculum to address the combined requirements of students at K-State and CGSC. At the same time, we will make the course materials modular so that they are extensible to be used at various other institutions. Our goal is to design the course material so that the courses could be taught independently, or could be broken into smaller parts (lesson plans), which can be interweaved/integrated at multiple points in existing courses where such knowledge is relevant.

b. Long-Term Benefits

The longer-term outcomes of this project include the following aspects:

(a) Increase in number of professionals with high-quality cybersecurity training,

(b) Increased interest in and awareness of cybersecurity,

(c) Enhanced faculty expertise in information assurance at participating organizations.

Our collaborations with CGSC will provide us with an excellent opportunity to design and evaluate innovative techniques to effectively deliver cybersecurity education to a diverse set of students. As a result, we envision that the impact of the proposed project will be much broader than the avenues identified above.

To ensure a broader impact of the curriculum material developed in this project, we will build upon and expand ongoing security curriculum, which will provide us an excellent platform to deliver our curriculum to a much broader audience. We will also reach to a number of other regional schools on sharing the curriculum for their students. Such an education effort will undoubtedly help improving the preparedness of the nation's

workforce for dealing with current cybersecurity challenges. CISA faculty engages in a number of outreach programs including NSF-funded Research Experience for Teachers and GK-12 STEM Fellows, Girls Researching Our World and ExCITE for middle school and high school girls, respectively, and the Developing Scholars Program. CISA members have been working with Harvard Townsend, Chief Information Security Officer at Kansas State University to carry out a series of activities to help raise awareness of both basic cybersecurity skills and more advanced technologies at K-State. We presented a demonstration of common exploits that could happen on personal computers.

3. Proposed Project Details

Our strategy is to develop the curriculum to address the combined requirements of students at both K-State and CGSC. At the same time, we will make the course materials modular so that they are extensible to be used at various other institutions.

We have engaged in discussions with curriculum leaders and security personnel at Command General and Staff College at Fort Leavenworth and the Office of Information and Technology Systems at K-State. As anticipated, together we have identified student categories requiring different levels of cybersecurity/information assurance education as outlined below:

- **End-users of computing devices:** This category corresponds to the general student population from a broad range of disciplines (such as arts, sciences, engineering, and agriculture) who use computing platforms primarily as consumers or producers of information. They require basic cybersecurity knowledge, such as how to protect personal and business information on a computing device, how to recognize and avoid attacks such as phishing and identity thefts, and how to safely access information available online.
- **Program coordinators – intermediate level users:** This category includes students whose studies and careers are dependent on cyber-infrastructure – they may manage information flow in their organizations, operate/maintain complex computing infrastructures such as applications, servers, and small networked systems, manage data collections (database or a file system) that may contain large amounts of data. These students are likely to be science, business, or engineering majors, but may not have had in-depth training in computer science. They will need a detailed but high-level understanding of security concepts to be able to safely and securely operate information systems to suit their job needs.
- **Advanced computer users:** This is the category of students whose major is computer science or engineering and whose future job responsibilities will likely involve software system design, programming, and project management. These students will need in-depth knowledge of fundamentals of information assurance and computer security.
- **System administrators and security engineers:** These are computer science or engineering majors specializing in cybersecurity, and their future job responsibilities will include protecting networked systems in an organization from cybersecurity threats. Their education needs for cybersecurity are more advanced compared to the other groups, and must learn not only cybersecurity fundamentals, but also cyber-offense and defense techniques to prevent attacks, recognize them when they happen, and recover from them if the attacks succeed.

The existing cybersecurity curriculum in the Computing and Information Sciences Department at K-State has been designed mainly to suit the needs of the ''advanced computer users" group or above. In the proposed work, we intend to leverage our faculty's expertise to develop a *comprehensive Homeland Cybersecurity curriculum* that can be used by a wide range of educational institutions to teach students with diverse educational backgrounds. This curriculum

will consist of a sequence of four courses, starting from an introductory security course and ending with team-based projects and competitions.

Based on the needs of the various student bodies, we have identified the following four courses in cybersecurity/information assurance that comprise the overall curriculum. Our goal is to design the course material so that the courses could be taught independently, or could be broken into smaller parts (lesson plans) which can be interweaved/integrated at multiple points in existing courses where such knowledge is relevant.

- **Course 1:** Introduction to information assurance and cybersecurity
- **Course 2:** Emerging threats in cyberspace
- **Course 3:** Advanced cyber-offense and defense technologies
- **Course 4:** Cyber-warfare.

Course 1 is intended primarily for the group "end-users of computing devices," who will benefit from basic understanding of computer security and how to achieve desired levels of information assurance. Course 2 is intended primarily for the group "program coordinators – intermediate level users," who will likely need to obtain up-to-date knowledge about current cyber-threats. Course 3 will be primarily targeted to the group "advanced computer users" as well as "system administrators and security engineers." consisting of computer network operators and system programmers, who will benefit from more in-depth technical knowledge in the area. Course 4 will be an exercise-oriented cyber defense/offense course wherein cyber attack competitions will be used so that the students can apply what they learn in Course 3 in the "battlefield."

4. Curriculum Development and Delivery to CGSC

The development and delivery of the curriculum will be managed collaboratively by a team consisting of the investigators of this project, a Program Coordinator at Kansas State University, Daniel Ward, Chief of Curriculum at the Command and General Staff College and Harvard Townsend, Chief Security Officer at Kansas State University. This team will collaborate on how the courses identified in the previous section will be integrated into existing curricula at CGSC and K-State. CGSC's current curriculum is divided into 15-week, 297-contact hour "Common Core" courses (shown as ILE CORE in Figure 1), followed by 16-week, 312-contact hour "Advanced Operations Courses" (shown as AOC in Figure 1), and 192-contact hour electives. We have found that the Common-Core and AOC courses are appropriate places to embed the materials in Courses 1 and 2. We plan to provide Courses 3 and 4 as electives to the students.

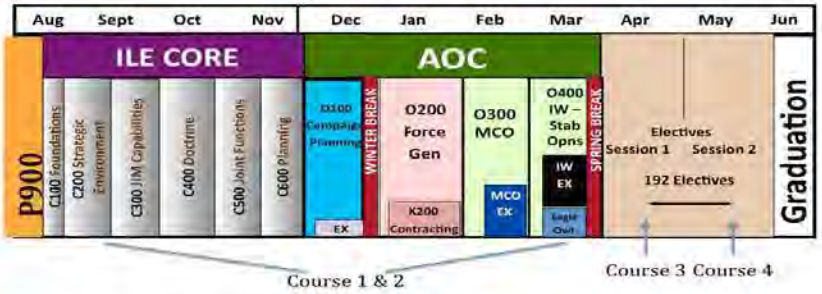


Figure 1: Course integration into CGSC curriculum

4

5. Project Timeline

K-State will closely work with CGSC in every phase of the project to ensure the developed curriculum can be effectively delivered in both K-State and CGSC classrooms. The following is a preliminary time line for the development and pilot-teaching of the courses.

1. Fall 2011: Regular meetings with CGSC personnel to understand their needs and existing curriculum structure.
2. Fall 2011: Create teaching materials for Course 1 and 2.
3. Spring 2012: Pilot teaching of Course 1 and 2 at K-State and CGSC.
4. Spring 2012: Create teaching materials for Course 3.
5. Summer 2012: Create teaching materials for Course 4.

6. Impact on the IASP Scholarship Program

The development of the proposed curriculum will impact the scholarship program in multiple ways. First, we plan to involve IASP scholars in the curriculum development process. The scholars will participate in the discussions of the content of Course 1 and 2. They will also have the opportunities to take part in pilot-teaching a few sessions as a way to practice their communication skills. Second, institutionalizing elements of this curriculum at K-State will not only help in broader cyber-security training, but also enable us to create a healthy pipeline of future IASP scholars. By exposing students to cyber-security early on in the program, we hope to attract a larger number of students. We plan to involve the IASP scholars in engaging with sophomores and juniors to create more interest in cyber-security and in preparing future IASP scholars. Without this curriculum, we find that students tend to commit to specialization in cyber-security either at the end of their junior year or beginning of their senior year. We feel that getting them interested in cyber-security as sophomores or first-semester junior will provide them a longer training period to develop advanced skills. In particular, Course 4 in the curriculum will help in team-building and put the acquired skills into practice.

7. Evaluation

Evaluation will be critical for the success of the project, and will be fully integrated into the various project activities. Our evaluation plan will be based on program goals and objectives to evaluate ongoing progress and provide feedback to the PIs and collaborators to maximize the project success. The evaluation will focus on (a) Assessment of lesson plans and projects, (b) Student performance, and (c) Assessment of the delivery mechanisms and the integration of security content into CGSC curriculum. A number of mechanisms such as needs analysis survey, class surveys and CGSC personnel feedback will be used throughout the project period.

8. Qualifications of the CAE-R to Meet the Project Objectives

Kansas State University has a long history of Information Assurance and Cybersecurity education and research. We have an extensive and advanced IA curriculum, including multidisciplinary courses with other departments on campus. Faculty members of CISA have been conducting world-renowned research in the information assurance and cybersecurity areas. We have a wide range of collaborations with industry and governmental agencies, and conduct a number of outreach activities in the IA/Cybersecurity area. These provide a solid platform on which we develop the proposed curriculum materials.

APPENDIX H

CYBER DOMAIN AND SCHOOL OF ADVANCED

MILITARY STUDIES CURRICULUM

School of Advanced Military Studies (SAMS)
Areas Addressing Cyber Domain

A. Morality and War Course -- Cyber Lesson

Lesson 5: Justice in War (The Dilemmas of Emerging Technology in War)

Dipert, Randall, R. (2010). "The Ethics of Cyberwarfare". *Journal of Military Ethics*, 9:4, 384-410. http://dx.doi.org/10.1080/15027570.2010.536404 (Read: pages 384-410) (16 pages).

Cook, James. (2012). "'Cyberation' and Just War Doctrine: A Response to Randall Dipert". *Journal of Military Ethics*, 9:4, 411-423. http://dx.doi.org/10.1080/15027570.2010.536406 (Read: pages 411-423) (12 pages).

B. Contemporary Operational Art (COA) Course & Cyber Lessons

Lesson 10: Space and Cyberspace

Gray, Colin S. 2005. *Another Bloody Century: Future Warfare*. London: Phoenix. [CARL: **909.83 G778a 2006**; read pages 291–330] [39 pages]

Zetter, Kim. 2011. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." *Wired* (11 July). [available here] [20 pages]

Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html

United States Department of the Army. 2010. *Cyberspace Operations Concept Capability Plan: 2016–2028* (February 22). [i–26; available here] [27 pages]

Libicki, Martin C. 2011. "Cyberwar as a Confidence Game." *Strategic Studies Quarterly*, vol. 5, no. 1 (spring): 132–46. [available here] [14 pages]

Klein, John J. 2004. "Corbett in Orbit: A Maritime Model for Strategic Space Theory." *Naval War College Review*, vol. 58, no. 1 (winter): 59–74. [available here] [15 pages]

Ellen Nakashima, "U.S. said to be target of massive cyber-espionage campaign," *The Washington Post*, 2/10/2013 http://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html accessed 2/11/2013 [3 pages]

GAO-13-462T, CYBERSECURITY: A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges [25 pages]
Verizon DBIR 2013 executive summary [10 pages]
[ref] CRS -- Cybersecurity: Authoritative Reports and Resources [100 pages]
[ref] Department of Defense Science Board, Resilient Military Systems and the Advanced Cyber Threat
[153 pages]

Lesson 11: Cyber II -- social media

Babak Rahimi (2011) "The Agonistic Social Media: Cyberspace in the Formation of Dissent and Consolidation of State Power in Postelection Iran", *The Communication Review*, 14:3, 158-178 [22 pages]
W. Lance Bennett & Alexandra Segerberg, Digital Media and the Personalization of Collective Action.[32 pages]
[ref] Social Network Analysis, A Brief Introduction
[ref] Role of the New Media in the Arab Spring Habibul Haque Khondker
Clicks, Cabs, and Coffee Houses: Social Media and Oppositional Movements in Egypt, 2004–2011 [23 pages]
Stanford study [74 pages]
Dempsey letter
151 pages

C. Engagement with ARCYBER POCs regarding appropriate learning objectives:
ARCYBER Proposed Cyber Learning Objectives:

ELO: Identify the five operational domains and describe the cyber domain relationship to the operational environment as a holistic aspect of decisive action and unified land operations.

TLO 1: Recognize the transformation the Cyberspace definition and its impact on Army doctrine and concepts.

TLO 2: Identify relationships between authority and boundaries as applied to Cyberspace across the joint command and control (C2) and US Army mission command (MC) constructs.

TLO 3: Identify the MC responsibilities of key organizations within the cyber community as they relate to Offensive Cyberspace Operations (OCO).

TLO 4: Recognize key Cyberspace adversaries, identify the categories of cyber threat actors, their key vectors and how they achieve effects in and through cyberspace.

SAMS leadership modified (Approved by COL Arnold-Director of SAMS) to fit within AMSP:

TLO: Explain the relationship between the cyber domain and the other operational domains in the conduct of unified land operations in the contemporary operating environment.

ELO 1: Analyze the impact of the new definition of cyberspace on Army doctrine and concepts.

ELO 2: Analyze the relationship between authority and boundaries under the joint command and control and US Army mission command constructs as applied to cyberspace.

ELO 3: Interpret the responsibilities of key organizations within the cyber community as they relate to Offensive Cyberspace Operations (OCO) under the mission command construct.

ELO 4: Identify the categories of cyber threat actors, key cyberspace adversaries, and how they achieve effects in and through cyberspace.

ARCYBER Executive Cyberspace Operations Planners Seminar (E-COPS). Students on orders following graduation (last May) for an ASCC level assignment attended the E-COPS delivered here at Ft Leavenworth. This was at the TS-SCI level and encompassed 8 US Army students. This seminar was intended to familiarize the students with Cyberspace Operations (CO) authorities, capabilities, organizations, policy considerations, and intelligence support to cyberspace operations planning; policies and procedures associated with requests and approvals for cyberspace operations capabilities; and lessons learned from recent and ongoing cyberspace operations.

APPENDIX I

CYBER LDE&T ASSESSMENT AND IMPLEMENTATION STRATEGY EXTRACT

UNCLASSIFIED

ARMY CYBERSPACE LEADER DEVELOPMENT, EDUCATION & TRAINING (LDE&T) ASSESSMENT & IMPLEMENTATION STRATEGY

1 JULY 2013
FINAL REPORT V0.9

APPROVED: 15 DECEMBER 2013

ARMY CYBER COMMAND
LEAVENWORTH SUPPORT ELEMENT
806 HARRISON DRIVE, BLDG 472
FORT LEAVENWORTH, KANSAS 66027-2326

UNCLASSIFIED

DEPARTMENT OF THE ARMY
ARMY CYBER COMMAND
FORCE MODERNIZATION PROPONENT
LEADER DEVELOPMENT, EDUCATION AND TRAINING DIVISION
8563 6TH ARMORED CAVALRY REGIMENT ROAD
FORT MEADE, MARYLAND 20755

ARMY CYBERSPACE LEADER DEVELOPMENT, EDUCATION AND TRAINING ASSESSMENT AND IMPLEMENTATION STRATEGY

OVERALL CLASSIFICATION OF THIS REPORT:

UNCLASSIFIED

PREPARED BY:
ARMY CYBER COMMAND
FORCE MODERNIZATION PROPONENT
FORT LEAVENWORTH SUPPORT ELEMENT
806 HARRISON DRIVE, BLDG 472
FORT LEAVENWORTH, KS 66027-2326

LDE&T Assessment and Strategy Point of Contact
Mr. Malcolm W. "Mack" Martin
Transformation & Technology Integrator
US Army Cyber Command
Fort Leavenworth Support Element
806 Harrison Drive, Building 472
Ft. Leavenworth, KS 66027
(913) 684-4600 office
(312) 552-4600 DSN
(301) 974-1079 BlackBerry
NIPR: malcolm.w.martin2.civ@mail.mil

SECTION 3: INSTITUTIONAL TRAINING AND SELF DEVELOPMENT DOMAINS

3. 1 Defining the Population

As mentioned in section 2.3, Methodology, this assessment looks at four sections; WHO, WHAT, WHEN and HOW as it relates to cyberspace related leader development, education and training. After assessing what currently exists, the data falls into the groups outlined. Section 3.2 breaks each group into greater detail:

WHO falls within the population requiring cyber-related training? Analysis has indicated that personnel can be broken into four categories. These are exclusive of the cyber-specific workforce.

a. **All Soldiers and Civilians**: Everyone who logs on to an Army network for whatever reason as a normal part of doing business or uses networked devices for communications, situational awareness, or survivability. This includes Army Reservists, Army National Guard, Civilians, contractors, and members of other Services.
b. **Leaders:** All Officers, Warrants and Noncommissioned Officers (NCO) and Civilians charged with leading, mentoring and developing junior personnel across the force.
c. **Staffs:** Specifically those members of a command group level, which carry responsibility for MDMP and support the commander's decision-making process. This also includes subject matter experts related to cyberspace operations.
d. **Commanders:** Those charged with the authority of formal leadership of units. This includes civilian leaders who are direct Army organizations and/or units.

Figure 3. Population Groups and Associated Shared Understanding Model

WHAT subject matter is unique to each group?

a. **All Soldiers and Civilians:** Require a level of digital literacy necessary to use their tools efficiently, productively, and securely. They must have the ability to identify a possible adversarial attack, perform initial actions, and report the incident.
b. **Leaders:** Require additional knowledge necessary to grow those in their charge, to mentor and develop effectively the next generation of Army leaders.
c. **Staff:** Must have subject matter expertise available regarding cyberspace capabilities and effects as part of the staff process for the benefit of the commander and rest of the staff.
d. **Commanders:** Need to have a baseline understanding of their unit's cyber-related vulnerabilities, as well as the cyber-related effects that may be leveraged against the adversary to help them in their mission analysis and operational planning process.

WHEN is the right point in a Soldier's career to introduce and reinforce cyber-related knowledge?

a. **All Soldiers and Civilians:** Initial Entry Training (IET) – for example, Basic Combat Training contains some non-combat topics of introduction, including Threat Awareness and Reporting Procedures (TARP) discussing foreign intelligence threats. Given the likelihood of exposure to the cyberspace threat, that would be an ideal time to introduce an awareness of the topic.
b. **Leaders:** Whether as a civilian, Soldier, NCO or officer, all personnel in leadership positions should receive "builds" of additional knowledge in order to lead competently. Beginning with Warrior Leaders Course (WLC) for NCOs, and with pre-commissioning for officers, digital literacy and the efficient use of software and applications, as well as increasing the defensive mind-set of their Soldiers, should be a continuing topic of reinforcement.
c. **Staff:** Officers going in to field grade staff and command roles receive advanced operational planning and integration during Military Education Levels (MEL) 3 and 4. Intermediate Level Education (ILE), School for Advanced Military Studies (SAMS) and other Services and joint schools and academies, must provide relevant cyberspace operational knowledge that allows for the inclusion of cyberspace into the operational planning process.
d. **Commanders:** In addition to the education received during MEL 4, commanders should be receiving additional knowledge regarding cyberspace operations, capabilities, and effects at the School for Command Preparation (SCP).

Figure 4. Cyber Training and Professional Military Education

HOW is cyber-related LDE&T currently delivered?

a. **Distance Learning (DL):** There are many opportunities to achieve a higher level of digital literacy through self development via the Army's Distributed Learning System (ADLS) capability leveraging Skillport. The education and training available via this method are free to all Soldiers and Civilians, and allow for an increasing capability and body of knowledge in all the common (and some not so common) cyberspace tools used by the community. The required annual training on Information Assurance Awareness (IAA) is conducted via DL. In addition to the ADLS offerings, the Joint Knowledge Online (JKO) portal offers a limited amount of DL opportunities. See Appendix 1 for a robust list of military, sister Service and joint cyberspace-related education and training websites.

b. **Resident/Institutional:** Outside the institutional education and training offered to those who require cyberspace specific or closely related knowledge, there really is no basic/foundational cyberspace institutional training in the Army today. This is expected,

given our current educating and training model for specific job skills within the institutional centers of excellence (CoE).

3.2 Population Groups and Specific Knowledge Requirements

All Soldiers and Civilians: Assessment of Current Soldiers and Civilians Cyberspace-Related Education & Training

To ensure Mission Command and the ability to support all operations, all Soldiers and civilians must be able to have access to the network and its information capabilities. The use of government information systems and access to government networks is a revocable privilege, not a right. However, unlike the vast majority of tools most individuals will ever touch, the actions and tools in the cyberspace domain can contribute to strategic effects on the most vulnerable portion of the Army Enterprise Infrastructure. All personnel play a role in the defense of Army networks and automation, whether they are infantrymen, supply sergeants, commanders, or mechanics. The Army's dependence on information technology requires all personnel to access computer systems and networks on a regular basis. With so many network users, an adversary can easily target hundreds of thousands of email addresses looking for vulnerabilities, and unbeknownst to that individual, potentially achieve catastrophic negative effects.

This section of analysis will focus on the general population who use and access the Army's network, but their jobs are not necessarily "cyberspace" related. This population group we consider the non-cyber workforce of the Army network. All Soldiers, Sailors, Marines, Airmen, Civilians and contractors whose role it is simply to protect their piece of the Army network defensive line by reducing the risks and vulnerabilities of their personal use.

As stated earlier, the digital literacy of all Soldiers and Civilians is an important factor in the efficient and secure use of the cyberspace domain. Army Digital Literacy (D-Lit) is individual awareness of attitudes toward and abilities to appropriately use digital tools to accomplish Army missions and personal and professional development.[13] D-Lit comprises a number of knowledge areas ranging from the basic ability to efficiently check and appropriately respond to email to an advanced level of word processing or spreadsheet applications. Contributing to the defense of the network, this analysis will focus on tactics, techniques and procedures (TTP) related to all D-Lit topics and the IAA activities, which can be rapidly implemented with minimal cost, provide a quantitative measure of effectiveness, and contribute to a less vulnerable cyberspace environment.

One-Time Education and Training

Soldiers attending Basic Combat Training receive minimal cyberspace operations knowledge. Within the standardized TARP– briefing, only three slides address the on-line threats of phishing/scams and data mining from social media/blogs. There was no other mention of cyber-related education or training in the course.

Lesson plans within the FA 29, Electronic Warfare Officer, and FA 30, Information Operations Officer, courses incorporate cyberspace overviews or fundamentals. The Military Intelligence CoE has incorporated cyberspace lesson plans for the counterintelligence agent (officers, warrants, and enlisted)

[13] Jane Mobley, "Study to Establish Levels of Digital Literacy for Soldiers and Leaders in the U.S. Army," 28 February 2011, pg 54

training, the warrant officer advanced course, and the signals intelligence/electronic warfare officer course. There is no other common-core cyberspace related education offered in the institutional training domain across the Army.

On-Going Education and Training

Currently, annual IAA training is the only cyberspace training/education required by the Department of the Army for all Soldiers and Civilians.[14] (DoD Cyber Awareness Challenge Training). Given the recent directives from the Secretary of the Army, Commander, US Forces Command (FORSCOM) and others, however, this annual training is not addressing the IA/Cybersecurity necessary to adequately protect the network.

On 1 February 2013, the Secretary of the Army (SECARMY) issued a memorandum stating that commanders are "responsible for the cybersecurity practices and compliance of their organizations, units would conduct an Information Assurance Self-Assessment, and that once-a-year training is simply not enough"[15]. The new DoD Cyber Awareness Challenge Training is a step in the right direction, but is not enough to address the issues adequately. The training focuses on three core awareness categories: local, mobile, and social (see Figure 5 below). To truly affect individual behavior, training must be personally relevant. The new training addresses personal on-line protection instead of simply focusing on the work environment. Additional training or awareness should include these three core awareness categories.

Figure 5. Core Awareness Categories (DoD Cyber Awareness Challenge)

Leaders: Assessment of Current Cyberspace-Related Leader Development and Education:

Soldiers and Civilians require training, education, and mentoring in order to become effective leaders. Part of the leadership development process is to impart to junior personnel the knowledge to conduct themselves in ways that limit their risks, personally and professionally, and physically and mentally. One area that has not received adequate emphasis is the area of cyberspace security. Leaders must be knowledgeable of those risks and their mitigations in order to communicate effectively to others, the potential dangers of operating in cyberspace. Similar to how the Army has traditionally dealt

[14] CJCSI 6510.01F, Information Assurance and Support to Computer Network Defense, Ch 5, 9 February 2011.
DoD Directive 8570.01, Information Assurance Training, Certification, and Workforce Management, Ch 4, 23 April 2007.
AR 25-2, Information Assurance, Chapter 2-8, 23 March 2009.
[15] Secretary of the Army Memorandum, Mandatory Information Assurance/Cybersecurity Awareness, 1 February 2013.

with operational security and TARP, leaders must be able to provide guidance on cyberspace threats, how social media can create vulnerabilities, how the cyberspace domain can be leveraged for intelligence collection and personal manipulation, and the various ways information networks can be attacked.

Non-Commission Officer Education System Schools

WLC is the initial course for preparing NCOs for leading other Soldiers. The course is non-MOS specific and the primary course topics include: Leadership, Training Management, Map Reading, Land Navigation, Drill & Ceremony, and Warfighting. Currently, there is no complementary topic in WLC's 22-day training schedule for cyberspace awareness.

Advanced Leaders Course (ALC) & Senior Leaders Course (SLC) are MOS-specific courses focused on refining job qualifications and higher leadership responsibilities. Training schedules for these courses vary extensively regarding topics and course duration. There is no standardized training focused on cyberspace awareness.

The Sergeants Major Course (SMC) educates senior enlisted leaders from our Army, sister Services, and allied militaries to be agile and adaptive senior noncommissioned officers through the study of leadership, unified land operations, and the application of Joint, Interagency, and Multi-National organizations in an era of persistent conflict. The SMC is the consummate institution that prepares them to execute at all command levels throughout the DoD. Following SMC, many sergeants major will assume senior enlisted positions in staff S3/G3 sections, and eventually advise commanders as command sergeants major at battalion and above commands. Currently, the course does not provide any level of exposure to cyberspace operations.

Warrant Officers Education System

Warrant Officer Candidate School (WOCS) is the 'pre-appointment' school for warrant officers. It does not contain any cyberspace related common core subject material.

Warrant Officer Basic Course (WOBC) provides technical certification in the new warrant officer's primary specialty. Outside of cyberspace specific and related specialties, WOBC contains no cyberspace related common core subject material.

Warrant Officer Advanced Course (WOAC) is a professional development course at the branch proponent school. As with the basic course, there is no common core cyberspace related subject material.

Warrant Officer Staff Course (WOSC) is a professional development course at the US Army Warrant Officer Career College, which provides intermediate level education and leadership skills. It is branch immaterial common core curriculum, and there is no cyberspace related subject matter.

Warrant Officer Senior Staff Course (WOSSC) Like the WOSC, but for CW4s and CW5s providing senior level education, knowledge, and leadership skills. It also is branch immaterial common core curriculum, and there is no cyberspace related subject matter.

Commissioned Officers

United States Military Academy (USMA). The Department of Electrical Engineering and Computer Science offers 12 cyberspace specific courses, which cadets can take as electives or required components of their degree program. There are, however, no required common core cyberspace courses for the entire cadet corps.

Reserve Officer Training Corps (ROTC). Currently, there is no cyber-related program of instruction (POI) included in the Military Science curriculum, which is necessary to complete the commissioning process. Given the academic nature of the environment, establishing a baseline of cyberspace awareness/defense should be easily accomplished.

Officer Candidate School (OCS) is an intense 12-week course designed to train officer candidates on the fundamental of leadership and basic military skills, instill Army values and leadership, and evaluate the candidate's leadership potential. OCS trains seven days a week and candidates are either former enlisted/NCOs or just completed Basic Combat Training as part of commissioning directly as an officer. There is no cyberspace operationally related curriculum in the course.

Basic Officer Leader Course (BOLC). The prevalent need of junior officers is focused on supporting cyberspace defense, leadership and mentoring of Soldiers under their charge. There is currently no existing POI within BOLC that provides the baseline knowledge necessary for junior leaders to exercise leadership and mentoring ability for cyberspace operations. Students should receive the same level of basic leadership and appreciation for operating in cyberspace as is provided to WLC and ALC students.

Captains Career Course (CCC). The majority of these courses consist of advanced branch-specific education, and preparation for company command within units exercising the functionality of the MOS. There is currently no curriculum covering cyberspace operations, staff planning and integrating in the common-core phase.

Staffs and Cyberspace Planners: Assessment of Current Cyberspace-Related Staff Education

Army Headquarters from battalion through corps have a need to incorporate the planning and inclusion of all military capabilities at their disposal. In order to successfully plan for and integrate a capability, however, the commander and staff require some level of subject matter expertise be available to provide guidance on the capabilities and implementation of any given tool. What follows is an assessment of current cyber-related education in common core or non-cyber workforce skills training.

Intermediate Level Education (ILE). Very little cyberspace training/discussion occurs in the current common core POI, however, the Department of Joint, Interagency, and Multinational Operations (DJIMO), Command & General Staff College, has proposed introducing cyberspace to the curriculum. This concept adds three electives to the curriculum, beginning with one at the unclassified level, which explores the basics of cyberspace operations, particularly as it impacts non-military organizations, and the strategic and operational effects possible through those targets. The other two electives will range from Unclassified – FOUO through the TS//SCI level. The Fort Leavenworth ARCYBER Proponent Support Element continues to work with DJIMO in developing these courses. Given the audience that receives this institutional training, ILE applies to the "Commander/Senior Leader" group as well.

1st IO Command's Basic Computer Network Operations Planners' Course (BCNOPC) is an 80-hour course, taught at the TS//SCI level, that prepares planners to integrate cyberspace operations into

command operations from the tactical through strategic levels of operation. Army officer and warrant officer graduates are awarded the N9[16] Skill Identifier/Additional Skill Identifier (SI/ASI).

1st IO Command's Executive CNO Planners Seminar (ECNOPS) is an 8-hour seminar that provides senior commanders and staff officers on general staffs with a broad overview of requirements for cyberspace planning, including authorities, policy, process, and related issues.

1st IO Command's Senior Leaders CNO Awareness Seminar (SLCNOAS) is a 3-hour seminar developed as a train-the-trainer course, that can be integrated into other training curriculum to foster an understanding of the challenges and requirements to conduct operations in the cyberspace domain. This seminar can be presented by a graduate of the BCNOPC or by 1st IO Command Training Division's CNO / Cyberspace Cadre.

1st IO Command's Cyber Fundamentals Course (on-line training). The intent of this course is to facilitate an understanding at the basic level of cyberspace concepts and to help provide awareness of technologies and the complexities associated with cyberspace.[17]

Joint Knowledge On-line offers the following self development cyber-related courses:

1) EUC 101-WPC Defensive Cyber Warfare Course
2) J3O P-US1101-Joint Staff Officer Cyberspace Operations Awareness Course
3) J3S T-US1220 International Legal Framework for Cyber Defense
4) J6S N-US299 CyberLaw 2 Course

Joint Network Attack Course (JNAC) is a 160-hour course training officers and NCOs. Course prepares graduates to effectively plan Computer Network Attack operations, to include an understanding of the appropriate authorities, Battle Damage Assessment, Review Approval Process, de-confliction, legal issues, targeting, weaponization and execution processes.[18] Graduates are awarded the N9 SI/ASI.

Joint C4I Staff and Operations Course offered by the Joint Forces Staff College is a 120-hour course sponsored by the Joint Staff J6 aimed at the joint C4I decision makers in the focus areas of Command and Control, Network Operations, Intelligence, Space Operations Support, Joint Interoperability and C4I Planning.

Joint Advanced Cyberspace Warfare Course is a 4-week course designed to give senior leaders advanced knowledge regarding cyberspace operations. It will not make a cyberspace subject matter expert or qualified planner, rather it provides in-depth knowledge regarding the joint use of cyberspace in the conduct of military operations. It does not require a technical background, but does provide some depth of technical subject matter.

Commanders: Assessment of Current Cyberspace-Related Command & Senior Leader Development and Education

Commanders and staff generally come from the same pool of individuals, and almost all commanders will also be or have been staff officers at various points in their careers. They all matriculate through the Officer Education System. The Captain's Career Course is the first institutional

[16] The N9 skills identifier is provided for graduates of both the Basic Computer Network Operations Planners Course and the Joint Network Attack Course. The differences between the courses, as well as the length differences, result in different levels of skill among the graduates. Therefore, the Army should consider assigning different ASIs for graduates of the two courses, depending on which course they attended.

[17] Email 1stiocmdtrainingsupport@mi.army.mil for enrollment instructions.

[18] https://www.mcis.usmc.mil/corry/SitePages/JNAC.aspx

training environment where officers will receive additional situational awareness regarding operations, capabilities, and effects in cyberspace. ILE is the second, follow on exposure, offering both core and elective levels of learning objectives. Personnel identified or selected for potential command positions will frequently also attend one or more advanced professional military education (PME) courses, identified below with their current scope of cyberspace education.

School for Command Preparation (SCP) and School of Advanced Military Studies (SAMS). SCP develops, educates, and supports U.S. Army Command Teams – field grade and company commanders, command sergeants major, first sergeants, and spouses – across the range of military operations alongside unified action partners to provide relevant and ready, joint enabled command teams to the joint force commander. SAMS educates the future leaders of our Armed Forces, our allies, and interagency at the graduate level to be agile and adaptive leaders who think critically at the strategic and operational levels to solve complex ambiguous problems. Neither SCP nor SAMS currently offer any cyberspace-related learning objectives in their respective curriculum.

Army War College/Senior Service College (AWC/SSC). The purpose of AWC at this time in our Nation's history is to produce graduates who are skilled critical thinkers and complex problem solvers in the global application of land power. Concurrently, it is their duty to the Army to also act as a "Think Factory" for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate on ground forces' role in achieving national security objectives. In resident AWC, there are at least six core courses and four electives that include either a block of instruction, or lesson, devoted to cyberspace operations and understanding the domain. The AWC Distance Education Program includes one core course and two electives including discussion of the cyberspace domain and vulnerabilities. Many of the resident courses also involve key leader briefings/lectures from USCYBERCOM, ARCYBER, 10th Fleet, and 24th Air Force. In the future, AWC will be reviewing their core curriculum to incorporate cyberspace-related knowledge in national security/defense, regional & theater development, theater campaign planning, and mission command/unit of command.

Department of the Army Civilians (DA-Civilians): Assessment of Cyberspace-Related DA-Civilian Leader Development, Education & Training

Because of changing roles and responsibilities of the Army Civilian Corps, civilian training and leader development programs have evolved during the past few years. Based on its established officer and NCO education systems, the Army implemented the Civilian Education System (CES) in 2007 to enhance Civilians' career-long professional and leader development. CES leadership courses are required for all Army Civilians.

The CES Basic, Intermediate, and Advanced Courses focus on leadership and business practices (Continual Learning, Flexibility, Integrity/Honesty, Interpersonal Skills, Oral Communication Skills, Problem Solving, and Resilience). None of the CES curriculum focuses on cyberspace-related topics, and there are no common-core cyber-related materials in any of the courses.

3.3 Institutional Training Domain Recommendations

This LDE&T Assessment and Implementation Strategy recommends immediate development of curriculum to be incorporated into the institutional training domain as required or core/common core POI which will establish a baseline of knowledge for all Soldiers and Civilians. Table 1 outlines the

minimum recommended changes, by level and institution, which should be considered for implementation as rapidly as possible. The following are a summary of the recommended strategy:

1. **Conduct cyber awareness campaign through "cyber-safety stand down" training or mobile training teams to Army units/posts**
2. **Implement on-line cyber awareness program with daily reinforcement through simple quizzes and phishing exercises to test all Soldiers and Civilians, and track metrics to assess unit readiness**
3. **Incorporate cyberspace awareness/basic defense training for initial entry personnel**
4. **Develop junior leader training to promote "cyber hygiene" across the entire Army**
5. **Institute staff planner training to support the integration of cyberspace capabilities into operations**
6. **Develop commander training to reinforce cyberspace's vital role in facilitating Mission Command and leveraging cyberspace capabilities in unified land operations**

3.4 Institutional and Self Development Domains Implementation Strategy

NEAR-TERM (6 months): All Soldiers and Civilians Cyberspace-Related Education, Training and Self Development

Near-term solutions are courses of action to be implemented quickly and are designed to rapidly bridge the gap between the identified needs and a sustainable shift in culture that produce an Army force baselined in D-Lit and cyberspace operations as fundamental to every aspect of operations. Balancing the requirement for rapid change with fiscal responsibility and budget constraints will ultimately dictate 'how' the recommendations are implemented. Potential solutions which address institutional and self development training include:

1. **A 'Cyber-Stand-down' whereby all echelons conduct mandatory IA/Cybersecurity training in mass in order to rapidly communicate the seriousness of the issue and the individual behaviors which contribute to the current state of protection. This would require the rapid creation of the POI.**
2. **Quickly implementing D-Lit Enabling Learning Objectives, especially IAA related during each login opportunity (as discussed further in the Maintenance section below).**
3. **Creating Mobile Training Teams (MTTs), Train the Trainer Teams (TTTs), and Virtual Training Teams (VTTs) to sweep across organizations and conduct detailed face-to-face (or virtual face to face through VTC capabilities) IAA training events, beginning with those tactical level units (Company-BCT) identified for upcoming rotations in support of contingency operations.**
4. **Require further on-line training, in addition to the DoD Cyber Awareness Challenge, via professional and self-development mechanisms (e.g. Skillport MS Office classes).**
5. **Immediately begin the process of developing appropriate or leveraging existing POI and curriculum and incorporating into existing institutional training events as outlined in Table 1, below.**

MID-TERM AND SUSTAINMENT (6-12 months): All Soldiers and Civilians Cyberspace-Related Education, Training and Self Development

Training and education on the safeguarding of data and the network is a continuous approach that reinforces behaviors and consequences. The 'way ahead' is to ensure an adequate and sustainable level of cyberspace defense behaviors define the culture, are taken into consideration in all planning and execution efforts, and become familiar to the entire population on the Army's network. Cyberspace awareness and the integration of cyberspace operations training should be incorporated throughout PME, as well as a daily cyberspace awareness program to reinforce behaviors. In 2012-13, the Cyberspace Training Initiative at USSTRATCOM implemented these IA/Cybersecurity awareness themes and is starting to see behavioral change in individuals.[19] An assessment strategy is paramount to track the measures of effectiveness regarding these awareness programs. Regular, on-going and effective sustainment training may consist of the following:

1. **Log-in script induced TTP, alerts. While logging in, personnel would see a box appear during boot-up that discusses helpful automation tips or informs them of current on-line threats. The individual must acknowledge the information by clicking a button to proceed. An alternative to a one-button dismissal is a second "for more information" button. This could provide quantitative data for commanders regarding the amount of additional knowledge their Soldiers and Civilians are seeking. Behind the script, the computer would continue to run its normal boot-up processes. This would require minimal operations and maintenance. The office overseeing these efforts would continuously update the TTP and alerts to ensure relevancy, thus greatly increasing IA/Cybersecurity awareness on a variety of D-Lit topics. This could be CSA driven, USCYBERCOM or USSTRATCOM delivered, and require minimal bandwidth impacts.**
2. **Weekly IA log-in script induced quizzes[20] and monthly phishing exercises. As part of logging on, personnel would be required to answer an information assurance question. The computer would continue to boot-up while they answer the question. If answered correctly, the question would disappear. If answered incorrectly, additional information would appear to explain the correct answer. Phishing exercises would test personnel on a regular basis. If individuals follow a suspicious hyperlink, a text box would announce the test and explain what the individual failed to identify. The success rates for these tests could also be used to rate a unit's information assurance level, and possibly as a metric on a commander's evaluation report. This strategy is similar to the TTP and alerts. It requires minimal development because USSTRATCOM has already delivered a pilot. This could be implemented at installation Network Enterprise Centers.**
3. **Monthly IAA assessments of log-in script quizzes, phishing exercises, and other quantifiable data points. As a metric for tracking unit awareness levels, data could be compiled by unit to show unit success rates and identify topics for additional training.**
4. **Leadership accountability mechanisms, such as evaluation report comments, or USR ratings. In conjunction with the measureable quizzes and exercises listed above, raters**

[19] Cyberspace Training Initiative Newsletter, February 2013.
[20] Cyberspace Training Initiative, USSTRATCOM, Daily Digit.

could establish realistic goals for subordinate leaders to achieve. This would reinforce the SECARMY guidance that commanders are responsible for information assurance throughout their organizations and possibly be incorporated into each unit's directed IA Self-Assessment. Tracking a unit's IA readiness level through USR reporting would emphasize the importance to all commanders.

5. **Institutional Training Recommendations. Army Regulation 350-1 dictates common mandatory training across the entire Army. Appendix 2 of this assessment shows institutional training currently required and the prescribed frequency of the training/education. Having a basic level of cyberspace awareness/knowledge requirement added to the regulation would support a portion of the suggested training listed below (Table 1). The HQDA, DCS, G–3/5/7, maintains centralized control over mandatory directed training requirements and reviews them biennially. Adding cyberspace awareness/knowledge would be similar to Electronic Warfare Training required across the institutional training domain.**

MID-LONG TERM (12-24 months): Cyberspace-Related Institutional Training Domain Strategy

The Army must embrace the requirement to provide the knowledge necessary to plan and integrate, as well as operate in the cyberspace domain. While there are POIs being developed to provide the necessary education, more must be done. Re-evaluating current POIs and updating to reflect the realities of the cyberspace threat and operational environment (OE) must begin immediately with a target implementation no later than FY15.

	School	Additional time	Knowledge Areas / Learning Objectives
Enlisted	BCT/AIT	2 hrs	Add "Foundations of Cyberspace Operations" to POI. Could combine into existing "general topics" (e.g. TARP). Include topics on cyber-related threat and defense of networked systems and sensors, including social networking and mobile/PED vulnerabilities.
	WLC	2 hrs	Add leader's role in mentoring to achieve behavioral patterns that add to defense of the network (information assurance) and identifying possible adversarial attacks.
	ALC/SLC	3-4 hrs	Add leader's role in mentoring to achieve behavioral patterns that add to defense of the network (information assurance) and identifying possible adversarial attacks. Provide additional impacts/examples of compromise & effects.
	SMC	8 hrs	Add an executive level cyberspace operations seminar (1st IO Command ECNOPS similar) to POI
Warrant	WOCS	2 hrs	Add "Foundations of Cyberspace Operations" to POI. Could combine into existing "general topics" (e.g. TARP). Include topics on cyber-related threat and defense of networked systems and sensors, including social networking and mobile/PED vulnerabilities.
	WOBC	3-4 hrs	Add leader's role in mentoring to achieve behavioral patterns which add to defense of the network (information assurance) and

			identifying possible adversarial attacks. Provide additional impacts/examples of compromise & effects
	WOAC	8 hrs	Add an executive level cyberspace operations seminar (1st IO Command ECNOPS similar) to POI
Pre-Commissioning	USMA	8 hrs	Add "Foundations of Cyberspace Operations" to core POI. Could combine into existing "general topics" (e.g. TARP). Include topics on cyber-related threat and defense of networked systems and sensors, including social networking and mobile/PED vulnerabilities.
	ROTC	3-4 hrs	Contracted cadets complete DoD Cyber Awareness Challenge training at least annually. MS VI (senior year) research project - cyberspace threats and vulnerabilities.
	OCS	2 hrs	Add "Foundations of Cyberspace Operations" to core POI. Could combine into existing "general topics" (e.g. TARP). Include topics on cyber-related threat and defense of networked systems and sensors, including social networking and mobile/PED vulnerabilities.
Commissioned	BOLC	3-4 hrs	Add leader's role in mentoring to achieve behavioral patterns which add to defense of the network (information assurance) and identifying possible adversarial attacks. Provide additional impacts/examples of compromise & effects
	CCC	3-4 hrs	Introduce cyberspace integration concept, cyberspace planning introduction (in conjunction with other general subjects - common core POI)
	ILE (CGSC)	8 hrs core + electives	Add an executive level cyberspace operations seminar (1st IO Command ECNOPS similar) to common core POI, remainder as electives
	SAMS	8 hrs	Add an executive level cyberspace operations seminar (1st IO Command ECNOPS similar) to POI (potentially leveraging ILE electives for this requirement)
	SCP	4 hrs	Add an executive level cyberspace overview seminar (1st IO Command ECNOPS similar) to POI
	AWC/SSC	8-24 hrs	Leverage ILE developed electives as core for resident course
DA-Civilians	CES Basic	2 hrs	Add "Foundations of Cyberspace Operations" to core POI. Could combine into existing "general topics" (e.g. TARP). Include topics on cyber-related threat and defense of networked systems and sensors, including social networking and mobile/PED vulnerabilities.
	CES Intermediate	3-4 hrs	Add leader's role in mentoring to achieve behavioral patterns which add to defense of the network (information assurance) and identifying possible adversarial attacks. Provide additional impacts/examples of compromise & effects
	CES Advanced	8 hrs	Add an executive level cyberspace operations seminar (1st IO Command ECNOPS similar) to POI

Table 1. Institutional Training Domain Curriculum and POI Implementation Strategy

BIBLIOGRAPHY

Books

The American Heritage Dictionary of the English Language. 3rd ed. Boston, MA: Houghten Mifflin, 1992.

Stanley, Elizabeth A. *Evolutionary Technology in the Current Revolution in Military Affairs: The Army's Tactical Command and Control System.* Darby, PA: Dianne Publishing Company, 1998.

Government Documents

The Armor School. *Program of Instruction for 17-0-A The Armor Officers Basic Course.* Fort Knox, KY: The United States Army Armor School, July 1956.

_____. *Program of Instruction for 17-0-3 The Armor Officer Advanced Course.* Fort Knox, KY: The United States Army Armor School, September 1956.

_____. *Program of Instruction for 17-A-C22 Armor Officer Career Course.* Fort Knox, KY: The United States Army Armor School, August 1961.

Army Cyber Command, Force Modernization Proponent. "Army Cyberspace Leader Development, Education And Training (LDE & T) Assessment and Implementation Strategy." Army Cyber Command, Leavenworth Support Element, July 1, 2013.

Department of the Army. Headquarters U.S. Army Training and Doctrine Command. Training and Doctrine Command Pamphlet 525-3-1, *The U.S. Army Operating Concept: Win in a Complex World 2020-2040.* Fort Monroe, VA: Government Printing Office, October 31, 2014.

Gates, Robert M. *Quadrennial Defense Review.* Washington, DC: Defense Department, 2010.

Headquarters, Department of the Army. *Leader Development Strategy.* Washington, DC: Government Printing Office, 2013.

_____. Army Doctrine Publication 1-02, *Operational Terms and Military Symbols.* Washington, DC: Government Printing Office, August 2012.

_____. Army Doctrine Reference Publication 6-22, *Army Leadership.* Washington, DC: Government Printing Office, August 2012.

_____. Army Doctrine Reference Publication 7-0, *Training Units and Developing Leaders*. Washington, DC: Government Printing Office, August 2012.

_____. Field Manual 1-02, *Operational Terms and Graphics.*Washington, DC: Government Printing Office, February 2015.

_____. Field Manual 3-38, *Cyber Electromagnetic Activities.* Washington, DC: Government Printing Office, February 2014.

U.S. President. *National Security Strategy of the United States*. Washington, DC: The White House, May 2010.

_____. "The Comprehensive National Cybersecurity Initiative." The White House, March 2010. Accessed October 5, 2014. http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf.

Journals/Periodicals

Ackerly, Bill. "Lawrence Says Everything is Network Dependent." *States News Service*, June 20, 2012.

Conti, Gregory, Michael Weigland, Ed Skoudis, David Raymond, Thomas Cook, and Todd Arnold. "Towards A Cyber Leader Course Modeled on Army Ranger School." *Small Wars Journal* (April 18, 2014). Accessed October 9, 2014. http://smallwarsjournal.com/jrnl/art/towards-a-cyber-leader-course-modeled-on-army-ranger-school.

Conti, Gregory, Michael Weigland, Ed Skoudis, David Raymond, Thomas Cook, Todd Arnold, and Daniel Ragsdale. *Towards a Cyber Leader Course: Not for the Weak or Faint of Heart* 1337, no. 3 (May 2014). Accessed October 13, 2014. http://www.westpoint.edu/acc/SiteAssets/SitePages/Reports/FULL_TCLC.pdf.

Dempsey, Martin. "Leader Development." *Army* 61, no. 2 (February 2011): 25-28.

Hernandez, Lieutenant General Rhett. Quoted in Jennifer M. McFadden. "Fires 2020: Land and Cyber." *Fires* (July-August 2013): 30.

Johnson, Captain Kristen M. "Remaking the Signal Captain-A New Training Equation For Success." *Army Communicator* 38, no. 1 (Spring 2013): 19-23.

Magnuson, Stew. "Cyber Labor Shortage Not What It Seems, Experts Say." *National Defense* (August 2014): 30-31.

McBride, Margaret. "Everyone Critical to Cyber Defense." *Fort Leavenworth Lamp*, October 2, 2014, A2.

McFadden, Jennifer M. "Fires 2020: Land and Cyber." *Fires* (July-August 2013): 30.

Seffers, George I. "U.S. Army Builds Cyber Branch One Step at a Time." *Signal* (April 2015). Accessed April 11, 2015. http://www.afcea.org/content/?q=Article-us-army-builds-cyber-branch-one-step-time.

Tsukayama, Hayley. "Cyber Attack was large-scale, Sony says." *Washington Post,* May 5, 2011. Accessed December 6, 2014. http://www.washingtonpost.com/blogs/faster-forward/post/cyber-attack-was-large-scale-sony-says/2011/05/04/AF78yDpF_blog.html.

Zetter, Kim. "Sony Got Hacked Hard: What We Know and Don't Know So Far." *Wired,* December 3, 2014. Accessed December 10, 2014. http://www.wired.com/2014/12/sony-hack-what-we-know/.

Online Sources

Sandra@F-Secure. "Computer Invaders: The 25 Most Infamous PC Viruses of All Time." Safe and Savy, March 21, 2011. Accessed October 29, 2014. http://safeandsavvy.f-secure.com/2011/03/21/25-infamous-viruse/.

Armor Branch Historian. "The Heritage of Armor-Horse Cavalry Roots." U.S. Army Maneuver Center of Excellence, November 25, 2014. Accessed March 1, 2015. http://www.benning.army.mil/armor/historian/.

Army Capabilities Integration Center. "What is DOTMLPF?" March 26, 2014. Accessed January 23, 2015. http://www.arcic.army.mil/AboutARCIC/about-dotmlpf.aspx.

Army Aviation. "Army Aviation Timeline." U.S. Army. Accessed March 1, 2015. http://www.army.mil/aviation/timeline/index.html.

Fort Gordon Public Affairs Office. "Army Cyber Branch Offers Soldiers New Challenges Opportunities." U.S. Army, November 24, 2014. Accessed March 28, 2015. http://www.army.mil/article/138883/Army_Cyber_branch_offers_Soldiers_new_challenges__opportunities/.

Hatfield, Egon. "Women's History Month: ENIAC, First Computer Programmers." U.S. Army, March 18, 2013. Accessed April 11, 2015. http://www.army.mil/article/98817/Women_s_History_Month__ENIAC__first_computer_programmers/.

History. "The Invention of the Internet." A&E Networks, 2010. Accessed March 28, 2015. http://www.history.com/topics/inventions/invention-of-the-internet.

Lee, Dave. "Shellshock: 'Deadly Serious' New Vulnerability Found." *BBC News*, September 25, 2014. Accessed December 6, 2014. http://www.bbc.com/news/technology-29361794.

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. "Brief History

of the Internet." Internet Society. Accessed April 11, 2015. http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

Merriam-Webster. "Point of View." *Merriam-Webster Dictionary.* Accessed August 18, 2014. http://www.merriam-webster.com/dictionary/point%20of%20view.

Milord, Mike. "Leader Development a Critical Part of Cyber Space Mission." U.S. Army, August 9, 2012. Accessed September 21, 2014. http://www.army.mil/article/85408/Leader_development_a_critical_part_of_cyberspace_mission.

United States Army Combined Arms Center. "School of Advanced Military Studies (SAMS)." U.S. Army, February 25, 2015. Accessed April 11, 2015. http://usacac.army.mil/organizations/lde/cgsc/sams.

U.S. Army Maneuver Center of Excellence. "IBOLC Course Curriculum." U.S. Army. Accessed January 24, 2015. http://www.benning.army.mil/infantry/199th/ibolc/.

_____. "IBOLC Mission." U.S. Army, December 10, 2014. Accessed December 23, 2014. http://www.benning.army.mil/infantry/199th/ibolc/content/pdf/IBOLC_Mission_Statement.pdf.

_____. "Officer Candidate School (OCS)." U.S. Army, March 6, 2015. Accessed April 9, 2015. http://www.benning.army.mil/infantry/199th/ocs/.

U.S. Department of Defense. *Department of Defense Cyberspace Workforce Strategy*. Chief Information Officer, December 4, 2013. Accessed October 13, 2014. http://dodcio.defense.gov/Portals/0/Documents/DoD%20Cyberspace%20Workforce%20Strategy_signed(final).pdf.

Wikipedia. "United States Army Aviation Branch." Wikipedia Foundation, July 17, 2014. Accessed March 28, 2015. http://en.wikipedia.org/wiki/United_States_Army_Aviation_Branch.

Your Dictionary. "Heinz Guderian Facts." LoveToKnow Corp. Accessed April 27, 2015. http://biography.yourdictionary.com/heinz-guderian.

Other Sources

Nickels, Marvin L. Subject: Command and General Staff Oficers Course (CGSOC) Electives Program Memorandum of Implementation (MOI) for AY2015. U.S. Army Command and General Staff College, Fort Leavenworth, KS, 8 December, 2014.

Cardon, Lieutenant General Edward General. Guest Speaker Lecture. U.S. Army Command and General Staff College, Fort Leavenworth, KS, December 3, 2014.

Doughty, Major Robert A. Leavenworth Papers No. 1, *The Evolution of US Tactical Doctrine 1946-76.* Fort Leavenworth, KS: Combat Studies Institute, August 1979.

Kansas State University. "DoD Information Assurance Scholarship Program." Annex II-Capacity Building, Technical Proposal-Project Name: Outreach to Department of Defense. Kansas State University, Manhattan, KS, 2011.

Norman E. Powell, Assistant Adjutant General. Memorandum, Subj: Program Change Proposal to Support Establishment of Aviation Officers Basic and Advanced Courses at the Aviation Center. Headquarters, U.S. Army Aviation Center, Fort Rucker, AL, January 10, 1979.

Odierno, General Raymond T. Cover letter, Army Doctrine 2015 publications, September 5, 2012.

_____. Keynote Speech, Association of the United States Army Annual Eisenhower Luncheon, October 23, 2013.

The Privacy Office, Homeland Security. "How to Safeguard Personally Identifiable Information." U.S. Department of Homeland Security, Washington, DC, May 2011.

Sullivan, General (Retired) Gordon R. Quoted in General Raymond T. Odierno. Cover letter, Army Doctrine 2015 publications, September 5, 2012.

U.S. Army Command and General Staff College. "C300 Lessons." Blackboard. Accessed December 22, 2014. https://cgsc.blackboard.com/webapps/portal/frameset.jsp?tab_tab_group_id=_2_1&url=/webapps/blackboard/execute/launcher?type=Course&id=_3204_1&url=.

_____. "C206 Theater Assessments and Strategic Estimates." Blackboard. Accessed December 22, 2014. https://cgsc.blackboard.com/webapps/portal/frameset.jsp?tab_tab_group_id=_2_1&url=/webapps/blackboard/execute/launcher?type=Course&id=_3096_1&url=.

Wenzel, Frank. "Developing Leaders." White Paper, Center for Army Leader Development, Fort Leavenworth, KS, 2013.